Sobreexposición Personal en la Red

"Cuando compartir es demasiado"

Escrito por: Leonel Erlichman

SOBREEXPOSICIÓN PERSONAL EN LA RED.

DE LO PRIVADO A LO PÚBLICO.

CUANDO COMPARTIR ES DEMASIADO.

Escrito por: Leonel Erlichman @leonele

"Sobreexposición Personal en la Red"

Autor: Leonel Erlichman

Libro Electrónico: **ISBN 978-9974-98-683-1**

Libro Impreso: **ISBN 978-9974-98-684-8**
Impreso por Bubok / Impreso em España

LICENCIAMIENTO:

Este libro se publica bajo licencia Creative Commons de tipo “Reconocimiento – No Comercial – Sin obra derivada”; se permite su copia y distribución por cualquier medio siempre que mantenga el reconocimiento de su autor, no haga uso comercial de la obra y no realice ninguna modificación de ella. La licencia completa puede consultarse en http: //creativocommons.org/

Sobreexposición Personal en la Red por Leonel Erlichman se encuentra bajo una Licencia Creative Commons Reconocimiento-NoComercial-SinObraDerivada 3.0 Unported.

ÍNDICE

1. Introducción. 8

El auge de la web 2.0 y la relación de nuestras vidas con la red han llevado a manejar la idea del Yo Digital como parte de nuestra identidad.

2. Identidad Social Online..... 16

Los fragmentos que conforman nuestra identidad en la web, como se relaciona con nuestra vida en el mundo físico y la influencia que esta ejerce.

3. Privacidad..... 30

El verdadero peligro es la gradual erosión de las libertades individuales a través de la automatización, integración e interconexión de sistemas pequeños y separados de mantenimiento de registros.

4. La red tiene memoria de elefante. 54

Con zettabytes de capacidad de almacenamiento, Internet es donde realmente nunca se olvida, es donde reside esa memoria colectiva con la capacidad de a largo plazo recordarlo todo.

5. La reputación 'online'. 66

Cada cosa que hacemos en la red así como cada contenido que publicamos contribuye a construir, configurar y reforzar nuestro branding personal, por lo que la gestión de la reputación online es una necesidad.

6. Seguridad de los jóvenes en Internet 78

La gran mayoría de los adolescentes hacen uso de Internet sin la correcta supervisión por parte de los adultos. Es necesario poner énfasis en la protección de datos personales, la educación y la seguridad.

7. Privacidad de datos personales en Facebook 88

En la red social con mayor cantidad de usuarios registrados y mayor actividad, nuestra seguridad es tan fuerte como la de nuestro amigo con la peor o más débil configuración de privacidad y seguridad personal.

8. Sobreexposición de Información..... 114

La red toca casi todos los aspectos de nuestras vidas, por lo que al compartir demasiada información personal en la web, bajo ciertas circunstancias o usos, nos puede resultar incómodo o inaceptable.

9. Fuentes de Información..... 134

Podría haber incluido la URL de cada informe o reporte leído, pero les dejo las URL de las fuentes principales, lo demás es hacer una simple búsqueda en estos sitios o en tu motor de búsquedas preferido.

1. INTRODUCCIÓN.

Desde hace un tiempo hemos visto con una celeridad increíble la masificación de una nueva forma de interactuar en la red, un fenómeno que se dio a conocer como la Web 2.0, con servicios o sitios cada vez más populares.

De todas las definiciones o explicaciones que he encontrado en la red o escuchado en disertaciones sobre esta idea originada por Tim O'Reilly, la que más me ha gustado o la que más comparto es la de Alberto Ortiz de Zárate Tercero quien en su libro de Blogs para Empresas explica a la Web 2.0 como "Un fenómeno social en relación con la creación y distribución de contenidos en Internet, caracterizado por la comunicación abierta, la descentralización de autoridad, la libertad para compartir y usar, dentro de un enfoque que trata a las relaciones humanas y económicas como conversaciones."

Una de las características o tendencias más interesantes que existen hoy en día en la Web, es la construcción casi compulsiva del Yo Digital de las personas, que se disemina y crece en forma exponencial en *blogs,* espacios de discusión y redes sociales del estilo de Facebook, Twitter, Google+, Foursquare, etc.

¿Qué tienen en común el mejor amigo de la infancia al que no vemos hace tiempo, un compañero de la universidad, el jefe y nuestra pareja? Si somos uno de los cientos de millones de personas que utilizan las redes sociales, hay una buena probabilidad de que estemos vinculados a ellos a través de una relación en línea. La información que compartimos con nuestros contactos nos permite mantenernos relacionados con ellos sin mucho esfuerzo. Pero, ¿quién más está mirando esa información? y ¿cómo puede utilizarla?

Podemos pensar que la unidad básica de una identidad online o identidad de Internet es un perfil de usuario, ese que cada uno establece en las distintas comunidades y/o sitios web; creándolo de forma que se nos identifique dentro de ellas. Mientras que algunos usuarios prefieren utilizar sus nombres reales, otros prefieren ser anónimos, o identificarse por seudónimos en los cuales revelar sólo una porción de información personal identificable. Estas diferencias y posibilidades varían de un sitio a otro o de una red social a otra.

Adicionalmente a estas definiciones, las redes sociales interactúan entre ellas mediante herramientas de terceros o por desarrollos propios de cada motor de red social, permitiendo que los usuarios manejen de esta forma la relación entre sus distintos perfiles en las diferentes redes, para ir construyendo un Yo Digital formado por su presencia en los sitios web, foros o blogs en los que participe.

Sin embargo, no podemos olvidar que muchas personas y/o empresas, además de amigos, compañeros de trabajo y conocidos están interesadas en la información que los usuarios suben en las redes sociales. Desde cobradores de deudas, reclutadores o empresas en busca de talentos, ladrones de identidad, estafadores, hasta empresas que buscan obtener una ventaja en el mercado utilizando redes sociales para recopilar información sobre los consumidores. Las empresas operadoras de redes sociales recogen una serie de datos sobre sus usuarios, tanto para personalizar los servicios que brindan a estos, así como para compartirlos con anunciantes.

Hay varios tipos de redes sociales, con distintas implicaciones de privacidad y seguridad en su utilización. La mayoría de estas combinan elementos de más de uno de estos tipos, y el centro o el objetivo principal de una red social puede cambiar con el transcurso del tiempo.

Las **redes personales** permiten a los usuarios crear perfiles detallados en línea y comunicarse con otros usuarios, con énfasis en las relaciones sociales como la amistad. Por ejemplo, Facebook, Friendster, etc. Estas redes a menudo involucran el compartir información con otros usuarios previamente autorizados, tales como ser género, edad, intereses, nivel educativo y el empleo, así como los archivos y enlaces a música, fotos y videos. Estas plataformas también pueden compartir cierta información seleccionada con otros usuarios y aplicaciones que no están autorizados como contactos.

Las **redes de actualización de estado** básicamente permiten a los usuarios publicar actualizaciones generalmente cortas, como ser el caso de Twitter. Han sido diseñadas para transmitir información rápidamente y en público, aunque puede haber configuración de privacidad para restringir el acceso a ellas o el acceso a las publicaciones.

Las **redes de ubicación** crecen con la llegada de los teléfonos celulares con GPS, y son cada vez más populares. Pensadas para transmitir la propia localización en tiempo real, ya sea como información pública o como una actualización visible a los contactos autorizados. Muchas de estas redes están diseñadas para interactuar con otras redes sociales, de modo que una actualización realizada a una ubicación de red puede, con la debida autorización, hacer una actualización posterior a otra de las redes sociales. Algunos ejemplos de redes de ubicación incluyen Brightkite, Foursquare y Google Latitude.

Por otro lado las **redes de intercambio de contenido** están diseñadas como plataformas para compartir contenidos como música, fotografías y videos, en forma pública o con contactos e interactúan con otros usuarios a través de comentarios. Algunas redes de intercambio de contenidos populares incluyen YouTube, Flickr y Picasa.

Las **redes de interés compartido** se construyen en torno a un interés común o dirigido a un grupo específico de personas. Estas redes incorporan características de otros tipos de redes sociales, pero se inclinan hacia un subgrupo de individuos, tales como

aquellos con aficiones similares, antecedentes educativos, las afiliaciones políticas, origen étnico, creencias religiosas, orientación sexual, etc. Algunos ejemplos de estas redes son LinkedIn, Negro planeta, Goodreads, Gay.com, etc.

Todas estas identidades online interactúan con otras y con la red en sí misma, de esa forma van adquiriendo una reputación asociada a ellas y que permite a otros usuarios poder decidir si la identidad es digna de confianza como para establecer una relación. Los conceptos de la autorrealización personal, y el cómo esta se ve influida por las nuevas tecnologías, son un tema de investigación en campos como la psicología y la sociología. El efecto de desinhibición online es un ejemplo notable, con referencia a un concepto de la conducta imprudente y sin inhibiciones que a veces suele presentarse en Internet. Es una verdad comprobable diariamente que las personas se comportan en la red de forma que normalmente no lo harían en un intercambio cara a cara, quizás por falta de habilidad en el manejo de una relación en la cual se pierden estímulos como los generados por cambios en el tono y la inflexión de la voz, los gestos y expresiones faciales y corporales, etc. Como sucede en nuestra vida, diariamente tratamos con personas de todo tipo, pero en una relación con interacción física podemos escoger dentro de un orden con quiénes relacionarnos, en Internet esto es más difícil dado que medio mundo está a un click de distancia.

Utilizamos todo este abanico de redes sociales a diario, algunas más que otras, generalmente sin considerar los riesgos que

nuestra actividad trae implícita, sin saber cuanta información personal junto con la que nosotros subimos es recogida y almacenada por estas plataformas, y muchas veces sin tener una idea clara de que por más que hayamos modificado todas las configuraciones de seguridad y privacidad, esto no significa que nuestra información esté completamente segura.

La existencia de un Yo Digital queda de manifiesto con mayor claridad en la frase del profesor del MIT William J. Mitchell, quién utiliza el planteamiento filosófico de René Descartes, base del racionalismo occidental, y la expresa como "**I link; therefore I am"** ("Enlazo, por lo tanto existo").

Las nuevas tecnologías nos imponen tener una identidad digital, afirma la socióloga holandesa Saskia Sassen. Disponer en Internet de un perfil profesional riguroso y conectado a personas destacadas del sector en el que uno trabaja, con las que mantenerse en contacto de forma regular es una práctica habitual, no como forma de búsqueda de empleo sino en la búsqueda de reputación y valoración. En un tiempo no muy lejano el no estar presentes en la red se irá convirtiendo en una versión moderna de ostracismo.

El Yo Digital es hoy en día una parte de nuestra identidad, una parte complementaria de nuestras vidas que cada vez cobra mayor importancia, nos relaciona con nuestro círculo de amistad, nos referencia con nuestros pares y refleja nuestra existencia en la red.

Se estima que para el 2015 habrá unos 15.000 millones de dispositivos conectados a la red. La Web entrará al hogar principalmente por el televisor, y otros aparatos se vincularán entre sí sin intervención humana. Es necesario conectarse para no ser ignorado, las tecnologías nos proporcionan las herramientas, las personas proporcionamos la conversación, la vida, el contenido y el sentido de ser y de pertenecer.

Las relaciones entre la vida pública y la privada están cada día más mezcladas, la frontera entre estos dos mundos es cada vez más una responsabilidad individual, depende de nuestras creencias, nuestra forma de ver la vida digital, nuestros prejuicios, y por lo tanto variará de persona a persona. Dónde ponemos ese corte, esa frontera, dónde está la línea que divide lo público de lo privado es un asunto de cada individuo, una línea que debemos trazar cada uno de nosotros en nuestra existencia en la red.

El Yo Digital es una parte de nuestra identidad, a la que no debemos dejar de atender.

2. IDENTIDAD SOCIAL ONLINE.

En filosofía, la identidad es aquello que hace a una entidad definible y reconocible, en cuanto a la posesión de un conjunto de cualidades o características que la distinguen de otras entidades. La persona es definida como un ser racional y consciente de sí mismo, poseedor de una identidad propia.

En Psicología, persona designa a un individuo humano concreto, abarcando tanto sus aspectos físicos como psíquicos para definir su carácter singular y único.

Al decir del Dr. Traver, la identidad es el sentido de continuidad en la experiencia de nosotros mismos, donde se incluyen los valores, las creencias y un sentido de pertenencia a una entidad supra individual, una experiencia compleja que incluye a la memoria, a la autoimagen, a la vivencia del tiempo y a las emociones y valores. La identidad es el pegamento de la conciencia, es aquello que mantiene unidas sus partes. Nuestra identidad es lo que nos diferencia de otros individuos, aunque esta nos haga muy parecidos los unos con los otros.

¿Quién soy en el mundo real? Mi nombre es Leonel, porque así lo eligieron mis padres, nací a principios del año 1973 en Uruguay. Estudié en una de las escuelas públicas de la ciudad donde vivía y cursé estudios secundarios también en un instituto público de la

misma ciudad; de las opciones de idiomas opté por estudiar francés dado que tomaba clases de inglés particular y al llegar a bachillerato me decidí por la orientación Ingeniería para realizar una carrera en ese campo. Estoy casado, tengo dos hijos, vivo en una ciudad pequeña a 50 kilómetros de Montevideo, la capital de la República Oriental del Uruguay, en una casa que perteneció a mi familia por siempre, y nuestra mascota es un perro dálmata. En el fondo de mi casa tengo un árbol limonero, tres rosales y alguna que otra planta. La jardinería es un pasatiempo que he adquirido para eliminar el estrés, distraer el pensamiento y descargar tensiones.

En lo que refiere a mi vida profesional soy Analista Programador, tengo un Postgrado de Especialización en Gestión de Servicios de TIC, he tomado cursos de Gestión de Proyectos y Marketing de Internet, entre otros. He participado de varios seminarios de distintas temáticas y considero que siempre debo estar aprendiendo algo nuevo. Como dice Alvin Toffler, un prestigioso escritor y futurista estadounidense, "Los analfabetos del siglo XXI, no serán aquellos que no sepan leer y escribir, sino aquellos que no puedan aprender, desaprender lo aprendido y volver a aprender". En ese escenario el aprendizaje debe ser continuo, constante y siempre partir desde cero. Trabajo en ANTEL, un Operador de Telecomunicaciones propiedad del Estado Uruguayo que presta principalmente servicios de telefonía fija, móvil y de datos. He realizado trabajos particulares siempre en el campo de las TIC y he dado cursos de capacitación en empresas acerca de diversas tecnologías y programas informáticos.

No soy una persona pública, y mucho menos algún tipo de celebridad, ni tengo un grupo de fans; por lo tanto toda esta información es o era conocida en mayor o menor medida por aquellas personas que están cerca de mí o dentro de aquellas comunidades que frecuento, familiares y amigos, vecinos del barrio, compañeros de trabajo e individuos con quienes eventualmente me he cruzado en la vida por uno o varios caminos recorridos.

Cada uno de estos grupos maneja una pequeña parte de la información personal, y solo aquella información que incumbe al grupo perteneciente. Pero como en toda teoría de conjuntos hay individuos incluidos en más de uno, formando uniones a partir de las intersecciones en esos grupos y la mezcla de información.

La web social o las redes sociales, representan un espacio en el que las personas exponen su identidad o parte de ella, manejando la posibilidad de expresar y exponer su identidad en un contexto digital social. Por ejemplo, la gente define explícitamente su identidad mediante la creación de perfiles de usuario en los servicios de redes sociales como Facebook, LinkedIn o en cualquier otro tipo de web social.

Mediante el uso de blogs y expresando opiniones en estas redes, definen de forma más tácita sus identidades, su forma de pensar o sus gustos, creencias y posiciones sobre distintos temas.

La divulgación de la identidad de las personas presenta ciertas cuestiones relacionados con la privacidad, y la revelación no

deseada de información personal. Esta divulgación en gran medida depende de nosotros mismos, los usuarios adoptan estrategias en estas redes sociales que les permiten controlar el nivel de la divulgación de su información personal, o por lo menos considerarlo de esa forma.

Para definir cual es mi identidad online, o que partes o perfiles definen diferentes aspectos de mi ser digital, tengo un usuario en Facebook desde donde conecto o mantengo contacto con información de carácter personal y mis relaciones de amistad. Mi usuario se puede acceder desde la dirección http://www.facebook.com/lerlichman. En Flickr o Picasa comparto fotos y videos en Youtube, comento las fotos y videos de otros usuarios y opino sobre estas o simplemente las catalogo.

En el sitio de la red social Linkedin, comparto mi información profesional y laboral, me mantengo en contacto con antiguos compañeros, con nuevos socios de negocios o simplemente con personas o grupos con intereses similares a los míos. Mi perfil público, el que es visible para todos se puede ver en http://www.linkedin.com/in/leonele. Allí actualizo mi currículo, capacitación, trabajos y proyectos que tengan relación con este mundo. Comparto experiencias con millones de personas a través de una vasta red que se integra a partir de mi primer nivel de contactos.

En Twitter actualizo y comento noticias, agrego opiniones, me contacto con el universo de usuarios. Mi usuario es @leonele, pero sobre todo escucho a otros usuarios y/o sigo conversaciones

de otros acerca de los temas que me interesan, participo de estas conversaciones e interactúo con el universo de Twitter, el "twttierverse".

Otra de las organizaciones de usuarios que aparecen en la red son las comunidades virtuales. Un aspecto positivo, y comúnmente discutido de estas comunidades suele ser el hecho de que la gente puede presentarse a si misma sin miedos de persecución, si se trata de rasgos de personalidad, comportamientos que son curiosos, o el anuncio de un componente de la identidad del mundo real que nunca antes ha sido anunciado. Esta libertad deriva en nuevas oportunidades para la sociedad en su conjunto, especialmente la capacidad de las personas para explorar los roles de género y la sexualidad de una manera que pueden ser inofensivas, pero interesante y útil para aquellos que realizan el cambio, están explorando o tienen algún tipo de inquietud o conflicto. La identidad en línea le ha dado a la gente la oportunidad de sentirse cómoda en una amplia gama de funciones, algunas de las cuales pueden ser los aspectos subyacentes de la vida del usuario que la persona no es capaz de desarrollar en el mundo real.

Los blogs, por su lado, permiten a una persona expresar sus opiniones en ensayos individuales, o como parte de un debate más amplio, creando un foro público para compartir sus ideas. Los Bloggers y los usuarios de blogs a menudo optan por utilizar seudónimos para proteger su información personal y obtener más libertad editorial para expresar ideas que podrían ser impopulares

con sus familias, empleadores, etc. El uso de un seudónimo y un enfoque prudente a la revelación de información personal, pueden permitir a una persona proteger su identidad real, pero hace que construya una reputación en línea usando un nombre que no es el suyo. Esto ha ido disminuyendo con el tiempo pero aún podemos observar esta situación en los usuarios cuando hacen comentarios en forma anónima o con seudónimos.

La creación de redes sociales en Internet como Facebook, Google+, Twitter, LinkedIn, etc. permite a la gente mantener una identidad online dentro de un contexto de superposición del mundo en línea y el mundo real. Estas son a menudo las identidades creadas para reflejar un aspecto concreto o mejor versión de sí mismos. Las representaciones incluyen imágenes, las comunicaciones con otros “amigos” y la pertenencia a grupos de la red. Controles de privacidad, sobre todo las limitaciones de las redes sociales, también forman parte de esta identidad online.

Bien, pero ¿qué relación hay entre nuestros Yo Digitales y las limitaciones del mundo real? Debemos comprender que la identidad en línea no puede estar disgregada de la identidad real y las limitaciones sociales que se imponen en el mundo real. Los efectos de la alfabetización y las aptitudes de comunicación que posea el usuario online, o la falta de estas aptitudes por parte del mismo, tienen la capacidad de formar una percepción online del usuario de la misma forma que se construye una percepción de las personas a través de un cuerpo físico en el mundo real.

Todas estas identidades sociales online o la multiplicidad de ellas, pueden tocar aspectos de esta percepción de nuestra identidad online con consecuencias negativas en el mundo real para algunas personas, dependiendo de la forma en la que se utilicen. Muchos usuarios están colgando en Facebook, Flickr, MySpace, Picasa o en cualquier otra red social fotos, comentarios, anécdotas, y muchas otras actividades o actitudes, que pueden de distintas formas construir una reputación negativa en algunos aspectos de la vida como el laboral o el académico, cosa que veremos más adelante.

A modo de ejemplo, cuando las empresas o los cazadores de talentos, que están muy activos en la red, realicen una búsqueda por su nombre quizás encuentren a esa persona en actividades sociales que no les agrade, esto puede inclinar la decisión hacia otro postulante; el curriculum de un individuo ya no tiene la importancia exclusiva de otrora, sino que ahora las personas son influidas por lo que la red y sus identidades en la red dicen acerca de ellos mismos. Hablaremos de esto en mayor detalle cuando comentemos de reputación online, mezclando de esta forma dos realidades que no siempre estaban unidas, la vida privada y la vida profesional.

Este aspecto roza un punto muy delicado de los individuos, la separación entre la vida íntima de las personas y la vida pública. Todas estas redes sociales, o mejor dicho, la forma en que estas son utilizadas por los usuarios, conspiran contra la privacidad de ellos mismos. Si algo es público no es privado. En este caso las

mezclas de la vida privada y la pública; así como la vida social y la profesional son una consecuencia negativa de todo este fenómeno.

Hace no mucho tiempo se pensaba que Internet era el lugar donde el anonimato prosperará, basado en la no identificación de los usuarios o hasta en servicios con avatares ficticios. Hoy en día la situación es diametralmente opuesta, ahora se considera que Internet ha pasado a ser el lugar donde el anonimato muere.

Para marcar un ejemplo, una persona que estaba en Nueva York comenzó a discutir con el conductor que la transportaba, durante la discusión se defendió argumentando sobre su educación "¿Sabes las universidades a las que he asistido y qué tan bien educada estoy?"

Fue identificada públicamente después de que se publicara en YouTube un video tomado por un teléfono celular sobre este encuentro. La mujer, que había asistido a la Universidad de Nueva York, fue ridiculizada por un grupo de bloggers por este hecho.

La inteligencia colectiva de dos mil millones de usuarios de Internet, y las huellas digitales que cada uno deja en los diferentes sitios, se combinan para hacer que todos los vídeos vergonzosos, todas las fotos íntimas, y cada e-mail con poca delicadeza pueda ser atribuido a su fuente originaria, ya sea que la fuente quiera o no que así sea. Esta inteligencia hace que la

esfera pública sea más pública que nunca, y a veces fuerza la vida personal y la lleva a la luz pública.

Esta comunidad o inteligencia colectiva funciona como un nuevo spider o bot o crawler, que no es un programa sino una comunidad de usuarios que recorre la web, no de forma metódica ni automatizada, pero sí estudia los contenidos, los indexa y cataloga, incluso agregando sus propios comentarios y valoraciones de cada uno de estos temas. A diferencia de los spiders tradicionales, este nuevo spider es humano, recorre la web a su gusto y utiliza criterios humanos para seleccionar, indexar, y comentar acerca los contenidos que encuentra.

La comunidad es inconmensurable, se manejan criterios humanos de selección, y esto ha hecho que cambiemos nuestros objetivos y pasemos de buscar información a buscar conversaciones acerca de esta información.

Cuando el fotógrafo independiente Rich Lam muestra sus imágenes de los disturbios en Vancouver de Junio de 2011 luego de un partido de hockey, se vieron varias tomas de un hombre y una mujer, rodeados por policías con equipo antidisturbios, en un beso de esos que se ven en las películas. Cuando las fotos se publicaron, se generó en la red una campaña que intentaba identificar a la "pareja besándose". Les llevó apenas un día a los familiares de la pareja el identificarlos y avisar a los sitios web de noticias sobre sus identidades, y allí estuvieron, en el programa "Today": Scott Thomas Jones y Alex, una prueba real de que gracias a Internet, nadie es anónimo. "Es un poco sorprendente

que hubiese alguien allí para tomar una foto", dijo Thomas en el programa televisivo.

Lo más probable es que esta pareja besándose disfrute de unos cuantos tweets de fama, de fotos que perdurarán en la red por siempre. Pero lo que hay que destacar es que fueron localizados con muchísima celeridad y precisión.

Esta destrucción paulatina del anonimato es producto de la generalización en el uso de redes sociales, cámaras fotográficas económicas y de teléfonos celulares inteligentes, los servidores de Internet que dan alojamiento a fotos y videos, y quizás lo más importante de todo, un cambio de mentalidad en la opinión de la gente sobre qué información puede ser pública y aquella que debería ser privada.

Se entiende que los sitios web como Facebook, que requieren o necesitan para un mejor funcionamiento de identidades reales y fomentan el intercambio de fotografías, vídeos y demás contenidos personales, han acelerado este cambio de mentalidad.

"Los seres humanos no quieren nada más que conectarse, y las empresas que nos están conectando electrónicamente quieren saber quién está diciendo qué y dónde" dijo Susan Crawford, una profesora de la Escuela de Leyes Benjamin N. Cardozo de la Universidad YESHIVA en Nueva York "Como resultado de esto, somos más conocidos que nunca."

Cada vez es más creciente esta vida pública, como se llama a veces, y viene con importantes consecuencias para el comercio,

para el discurso u orientación política y para el derecho de la gente común a la privacidad.

Algunos gobiernos están realizando diferentes esfuerzos junto con empresas para establecer sistemas de identidad en línea. La tecnología y su constante avance desempeñarán un papel aún mayor en la identificación de las personas anónimas en la red. Facebook, por ejemplo, está utilizando una tecnología de reconocimiento facial para las fotos de los usuarios que ha despertado alguna alarma en autoridades europeas.

Después de los mismos disturbios ocurridos en Vancouver que comentamos con anterioridad, la gente no necesitó de tecnología de reconocimiento facial para identificar a algunas personas, simplemente recorrieron los sitios de medios sociales para tratar de identificar algunos involucrados, como lo que sucedió con Nathan Kotylak de 17 años, un jugador estrella en el equipo junior de waterpolo de Canadá.

En Facebook, el Sr. Kotylak debió pedir disculpas por el daño que había causado. Pero el dedo señalador no solo lo afectó a él, sino que también afectó a su familia; medios de comunicación locales informaron que su padre, médico de profesión, habría visto reducida su calificación en un sitio de práctica de revisión médica RateMDs.com, después de los comentarios publicados sobre la participación de su hijo en los disturbios. Como la red funciona en ambos sentidos, luego de esto otras personas usuarias de Internet se dirigieron al sitio web para defender al médico y su reputación, y así mejorar su ranking nuevamente.

Como era de esperar, hubo una reacción a la identificación de Internet con ayuda de las personas involucradas en los disturbios. Camille Cacnio, un estudiante de Vancouver, que fue fotografiada durante el motín y que admitió haber participado en un robo, escribió en su blog que "la caza de brujas del siglo 21" en Internet es "otra forma de acoso moral."

Aunque el usuario que originalmente publicó el video de la persona que comentamos con anterioridad (objeto de burla en Internet por su discusión con un conductor en Nueva York), lo eliminó; la gente rápidamente había republicado el enlace y el video en si, dándole nueva vida a la historia y nuevos comentarios; a la semana siguiente decidió cerrar sus cuentas en Twitter y LinkedIn luego de que su nombre se repitiera en los blogs con demasiada asiduidad.

A medio mundo de distancia de allí, en países de Oriente Medio como Irán y Siria, los activistas han tenido éxito algunas veces en la identificación de las víctimas de la violencia dictatorial de sus gobiernos utilizando videos de YouTube cargados anónimamente.

La “Vida Pública”, algo que normalmente asociábamos sólo con personas famosas, ya no es escasa ni tiene tantas restricciones, debido a que la red no olvida ni las imágenes ni los momentos del pasado, como una explosión en un tren o un beso durante un motín. La realidad de un mundo público es un tema ineludible para todos, y del que vamos a escuchar mucho más, del que no podemos escapar y un hecho que deberíamos contemplar cuando decidimos tener una participación en la red.

Cerrando el tema, trataremos de comentar algo sobre la propiedad de la identidad online o la propiedad intelectual de los contenidos que estos usuarios suben y comparten en la red.

Una identidad online que ha adquirido una excelente reputación adquiere un valor importante principalmente por dos razones: en primer lugar, por el esfuerzo y el tiempo invertido en crear y construir ese usuario y dotarlo de dicha reputación; y en segundo lugar porque otros usuarios antes de realizar transacciones observan la identidad y su reputación para tratar de decidir si es suficientemente digno de confianza.

Ya no nos resulta sorprendente que alguna identidad online o avatar se ponga a la venta en sitios de subastas. Todo esto trae aparejado conflictos sobre la propiedad de estas identidades.

Hace un tiempo encontré un artículo sobre un usuario de un juego online llamado EverQuest. El juego y su sitio son propiedad de Sony Online Entertainment, Inc. Esta persona intentó vender su identidad Everquest en eBay. La compañía se opuso, afirmado sobre el carácter de propiedad intelectual de Sony y exigió se retirara la subasta, en los términos de la Digital Millennium Copyright Act (DMCA). EBay podría haber pasado a ser parte en un pleito de infracción de derechos de autor.

Quedando sin resolver, este asunto se transformó en una cuestión fundamental: ¿quién es el propietario de una identidad online creada en un sitio web comercial? ¿La identidad online

pertenece a la persona que la creó o a la empresa que posee el software utilizado para crearla?

A Facebook por ejemplo, sobre el contenido protegido por derechos de propiedad intelectual, como fotografías y videos de usuarios, se le concede a esta red social una licencia no exclusiva, transferible, con posibilidad de ser sub-otorgada, sin royalties, aplicable globalmente; pudiendo entonces utilizar cualquier contenido de este tipo que se publique por parte de sus usuarios. Solamente al eliminar un contenido o una cuenta este permiso se cancela, a menos que el mismo se haya compartido con terceros y éstos no lo hayan eliminado.

Esto incluye a las aplicaciones o a las empresas que desarrollan aplicaciones (más adelante hablaremos sobre la seguridad en Facebook y las configuraciones de privacidad).

3. PRIVACIDAD

La privacidad puede ser definida como el ámbito de la vida personal de un individuo que se desarrolla en un espacio reservado y debe mantenerse confidencial. La vida pública, por otro lado, es aquella porción de tu vida que le muestras al mundo, la que todos pueden ver, pero la vida privada son las cosas que vives o compartes contigo mismo, tu familia o tu núcleo más íntimo. Según el diccionario de la Real Academia Española, **privacidad** se define como "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión" e **intimidad** se define como "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia".

El desarrollo de la Sociedad de la Información y la expansión de la Informática y de las Telecomunicaciones plantean nuevas amenazas para la privacidad que han de ser afrontadas desde diversos puntos de vista: social, cultural, legal y tecnológico. La privacidad en Internet se refiere a controlar quien puede tener acceso a la información que posee un determinado usuario que se conecta a la red.

Un aspecto importante de Internet, es la neutralidad de la red. De su definición en Wikipedia se extrae que “una red neutral es aquella que está libre de restricciones en las clases de equipamiento que pueden ser usadas y los modos de

comunicación permitidos, que no restringe el contenido, sitios y plataformas…". Vint Cerf, co-inventor del Protocolo de Internet, ha asegurado que "Internet se diseñó sin ningún guardián sobre nuevos contenidos o servicios. Se necesita una regla de neutralidad de red suave pero aplicable para que Internet continúe creciendo", por lo que se entiende que nadie puede poseerla ni es posible controlarla. Esto influye mucho en el grado de apertura de la red y en el valor de Internet, pero también deja muchos puntos a juicio del propio usuario, tanto para los emisores como para los receptores de información. La privacidad en Internet dependerá del tipo de actividad que se realice. Las actividades que de antemano un individuo puede suponer son privadas en realidad no lo son, no existe ninguna actividad ni configuración de equipos o servicios en línea que garanticen la absoluta privacidad de los usuarios y de su información. Un ejemplo serían los registros de un nombre de dominio, ya que muchas personas obtienen su propio sitio en Internet y toda la información necesaria para realizar estos registros es pública y está al alcance de cualquiera, nombre, dirección, teléfonos, etc.

Esto no es algo que nace hoy con Internet y las redes sociales, la comisión para el estudio de la protección de la privacidad de los EE.UU. declaró en 1977 que el verdadero peligro es la gradual erosión de las libertades individuales a través de la automatización, integración e interconexión de sistemas pequeños y separados de mantenimiento de registros, cada uno de los cuales por sí solos pueden parecer inocuos, incluso benevolentes, y justificados en su totalidad.

Gran parte de los usuarios piensa que al navegar por Internet lo hacen en forma anónima al no acceder a ningún servicio con usuario y clave, pero en realidad esto no es así. Prácticamente todo lo que se transmite por Internet puede archivarse, incluso los mensajes, los archivos que consulta y las páginas que se visitan, mediante dispositivos como cookies, los navegadores, y los sistemas de analítica web. Los proveedores de acceso a Internet así como los sitios web tienen la capacidad de recopilar dicha información.

La interconexión de las distintas redes a Internet se hace en forma voluntaria, por lo tanto ninguna de estas controla Internet. Ésta es una red de comunicaciones de cobertura mundial que posibilita intercambiar información entre ordenadores situados en cualquier parte del mundo, y podemos decir que lo que se publica en Internet es de dominio público. Para acceder a toda esta información solamente es necesario un navegador web, que puede ser utilizado en muchos tipos de dispositivos diferentes, desde una PC, un móvil y hasta una consola de juegos.

Las personas generamos en la red mucha información y alguna de ella sin tener conocimiento de que está allí. Pensemos que existen básicamente dos tipos de información que se pueden obtener públicamente acerca de un usuario; la información que este comparte por sí mismo y la información obtenida o recopilada a través de métodos de seguimiento electrónico.

Dentro de la información que un usuario comparte por decisión propia se incluyen fotos y otros medios de comunicación

multimedia, edad y sexo, datos biográficos como educación, historia laboral, ciudad natal, etc., actualizaciones de estado, información de contactos o amigos, intereses y ubicación geográfica. Si bien podemos elegir como compartimos parte o toda esta información, ya sea como "pública" sin restringir el acceso a través de ninguna configuración de privacidad que esté disponible, también podemos hacerlo en forma privada cambiando la configuración de la red social, pero siempre cierta información puede ser visible al público de forma predeterminada. En algunas situaciones un usuario puede ser capaz de cambiar la configuración de privacidad para que su información sea privada o el nivel de privacidad sea mayor, de modo que sólo los usuarios autorizados puedan verla, pero siempre hay una porción de información que seguirá siendo pública, dado que no tenemos la opción de restringir el acceso a ella de manera total.

Debemos considerar que una red social puede cambiar su política de privacidad en cualquier momento sin el permiso de un usuario y sin que éste siquiera se entere. El contenido que se envió con determinada configuración de privacidad puede llegar a ser visible cuando una política de privacidad se ve alterada. Algo de esto ha sucedido con los servicios de Google que unificaron todas sus políticas de privacidad y generaron un único y gran repositorio de información de los usuarios unificando la información de los distintos servicios de la empresa.

Escapa a nuestro control la forma de actuar o compartir de nuestros contactos o amigos, estos pueden copiar y publicar la

información, etiquetarla, republicarla incluyendo fotos, videos, cometarios o simplemente usarla como propia con una restricción de seguridad menos rigurosa, lo que podría hacer un bypass a la configuración de privacidad original del contenido como veremos más adelante en el caso de Facebook.

Una aplicación de un tercero que ha tenido acceso al perfil de un usuario puede ser capaz de ver la información de este o de sus contactos e inclusive algunas veces la información que estos manejan como privada. Las redes sociales en sí no garantizan necesariamente la seguridad de la información que se ha subido a un perfil, aun cuando esta se haya definido como privada.

Otra forma de obtener información es a través de métodos de seguimiento electrónico. Es posible conseguir información en línea de un usuario mediante la acción de las "cookies". Para esto los sitios web que un usuario ha visto utilizan lo que se conoce como cookies de seguimiento, de forma de almacenar la información asociada a sitios web específicos (tales como artículos en un carrito de compras) para seguir el movimiento de un usuario de un sitio a otro así como para la construcción de un perfil en torno a un usuario.

De hecho, un estudio del año 2009 realizado por AT&T Labs y Worcester Polytechnic Institute encontró que el código único de identificación asignado a los usuarios de redes sociales puede ser emparejado con el comportamiento seguido por las cookies. Esto significa que los anunciantes y otros posibles interesados en estos datos son capaces de utilizar la información obtenida a través de

las redes sociales para construir junto con la información recogida por cookies un perfil de la vida del usuario, incluyendo los hábitos de navegación.

¿Quiénes tienen acceso a la información que publicamos en las redes sociales? Probablemente todos esperan que sólo sus contactos autorizados puedan verla, pero realmente ¿quién más puede ver esta información? y ¿qué datos son visibles exactamente?

Entre las entidades que recopilan información personal para fines legales se incluyen a los anunciantes, interesados en la información personal de cada individuo de modo de poder orientar mejor sus anuncios hacia éstos, así como desarrolladores de software de otros fabricantes que incorporan información para personalizar sus aplicaciones, como ocurre con los juegos en línea que interactúan con las diferentes redes sociales. También hay entidades que recopilan información personal para propósitos ilegales como robo de identidad u otros crímenes en línea, que obtienen información personal ya sea sobre la base de lo que un usuario publica o lo que otros postean acerca de esta persona.

Las redes sociales ofrecen sus servicios sin el cobro de ninguna tarifa a las personas que las usan, y obtienen beneficios entre otras cosas mediante la venta de publicidad dirigida a sus usuarios. Esto se suele hacer a través de la publicidad del comportamiento, también conocido como orientación o publicidad orientada. La publicidad del comportamiento es el término

utilizado para describir la práctica de la adaptación de los anuncios a los intereses personales de un individuo, para lo cual deben contar con mucha información personal y de hábitos del mismo. Esta práctica es atractiva para los comerciantes porque los anuncios dirigidos tienen más probabilidades de resultar en una compra por que anuncios no orientados. Este tipo de publicidad también suele ser valiosa para las redes sociales, ya que pueden ser vendidos anuncios a un precio más alto que los anuncios regulares, o resultar más interesante para los anunciantes aparecer en estos sitios.

Las redes sociales y otros gigantes de la red como Google recogen una gran cantidad de información sobre nosotros como clientes potenciales, que los anunciantes están muy interesados en utilizar. En cierto modo esto puede ser útil para el usuario debido a que los anuncios que visualiza parecen ser más relevantes, pero hay varios motivos de preocupación relativos a la publicidad de comportamiento. Los consumidores pueden no ser conscientes de que los datos se asocian con sus perfiles, y pueden no ser capaces de ver esos datos asociados a sus perfiles para corregir posibles errores o inconsistencias en la información recogida por las empresas. No hay períodos estipulados para máxima retención de los datos y no hay requisitos de seguridad para la conservación de los mismos, dejándolos susceptibles a los piratas informáticos y adicionando nuevos riesgos de seguridad. Tampoco existen restricciones sobre la edad de los usuarios; la información sobre los usuarios menores puede ser recogida y

utilizada para su posterior uso en dirigir publicidad de comportamiento.

En el contexto de las redes sociales, las aplicaciones de terceros son programas que interactúan con la red social sin ser parte de ella. Estas aplicaciones toman muchas formas, pero incluyen algunas típicas y populares como juegos, encuestas o software de diverso tipo para agregar funcionalidades a los usuarios. Las redes sociales permiten a los desarrolladores acceder a su plataforma con el fin de crear estas aplicaciones, de forma de hacer su red a través de estas aplicaciones sea más atractiva para sus usuarios y facilitando el desarrollo de nuevos métodos y formas más creativas de interactuar con los contactos y con la red en si.

Para realizar estas aplicaciones, las redes sociales permiten a los desarrolladores tener acceso automático a la información pública de los usuarios y adicionalmente las aplicaciones de terceros pueden acceder a cierta información privada de los mismos. Un usuario puede conceder un acceso a las aplicaciones de terceros para su perfil sin darse cuenta de la magnitud de los permisos de dicha concesión. Los usuarios también pueden asumir erróneamente que las aplicaciones de terceros utilizan los mismos estándares de seguridad que la red social que la contiene y dentro de la que se ejecutan, cosa que no siempre sucede como veremos más adelante tomando el caso particular de Facebook.

La mayoría de las redes sociales no asumen responsabilidad de las aplicaciones de terceros que interactúan con sus sitios.

Generalmente los permisos asignados por los usuarios les permiten acceder a más información que la necesaria para llevar a cabo sus funciones, permitiéndoles reunir una cantidad de datos de nuestros perfiles. Estas aplicaciones de terceros pueden acceder a la información general que se considera pública sin el consentimiento explícito del usuario, y a la que se considera privada cuando el usuario concede el permiso a dicha aplicación, cosa que ocurre al activar o habilitar la aplicación en nuestro perfil de usuario. Cuando cargamos una aplicación por primera vez el botón que presionamos para hacerlo dice “Permitir”, y justamente eso es lo que hacemos; le permitimos acceder a cierta información. Muchas de ellas incluyen una posibilidad para tener acceso a la información personal de los contactos de los usuarios sin que estos contactos hagan una concesión de permiso explícito, esto esta viéndose modificado con cambios en la seguridad que las redes sociales están implementando.

Otro punto de posible escape de información se da en el uso que harían el Gobierno y la Justicia de la información ubicada en las redes sociales. Pondremos como ejemplo lo que sucede en los Estados Unidos: la Ley de Libertad de Información (FOIA por su sigla en inglés) establece el proceso por el cual todo individuo puede solicitar acceso a registros o información de las agencias federales; valiéndose de esto las solicitudes presentadas por Electronic Frontier Foundation (EEF) con la asistencia de la Universidad de California-Berkeley, que han permitido que tengamos una visión más clara sobre cómo las agencias gubernamentales utilizan los sitios de redes sociales para sus

investigaciones, cómo realizan la recopilación de datos y la vigilancia de los usuarios. Aunque no son completos los documentos que han sido publicados, estos indican que las agencias gubernamentales, incluido el Departamento de Justicia de EE.UU. o el Servicio de Rentas Internas (IRC), han desarrollado materiales de capacitación interno instruyendo al personal sobre cómo utilizar la información del perfil público de un usuario en los sitios de redes sociales durante las investigaciones.

Cuando hablamos del acceso a la información que no es pública, cada red social ha adoptado sus propios procedimientos para tramitar las solicitudes que le llegan por vías legales de las agencias del gobierno. El grado en que estos sitios cooperan o no con la aplicación de la ley no puede ser plenamente explicado en las políticas de privacidad. En realidad el derecho primario es el de proteger la privacidad de la información en Internet. La Electronic Communications Privacy Act, permite a los funcionarios del gobierno acceder a la información en redes sociales solamente a través de una citación, para lo que los funcionarios de gobierno deben obtener un permiso para acceder a los datos. Un análisis de la base de datos judicial Westlaw realizado por Reuters, muestra que desde el año 2008 al 2011, los jueces federales otorgaron permiso para al menos 24 registros en las cuentas individuales en Facebook. Las agencias federales que solicitaron permisos incluyen al FBI, la DEA (Drug Enforcement Administration) y el servicio de inmigración y control de las fronteras de los EE.UU. El análisis de los datos Westlaw indican

que las instituciones federales recibieron al menos 11 permisos para obtener los datos de Facebook a principios de 2011, casi el doble del total calculado para el año 2010. El número exacto de permisos es difícil de determinar, en parte debido a que algunos registros son confidenciales, porque las peticiones oficiales a menudo son difíciles de identificar. En una entrevista realizada por Reuters, el vicepresidente de seguridad en Facebook Koe Sullivan, se negó a revelar datos sobre los accesos a la información por parte de las autoridades. Argumentó que en Facebook se mantenía la confidencialidad y la privacidad de los usuarios y que a menudo esto va en contra de los esfuerzos que las autoridades realizan en la búsqueda de información.

Otro punto de discusión es la utilización por parte de individuos o instituciones de la información ubicada en las redes sociales como pruebas en juicios penales y civiles. Esto incluye los juicios de divorcio, batallas de custodia de menores, demandas de seguros, los juicios penales y los casos presentados por la policía contra los estudiantes universitarios por comportamiento inadecuado o consumo de alcohol, por nombrar algunos.

El anonimato en las redes sociales no es una cuestión de malas prácticas, como algunos intentan marcar; muchos usuarios de redes sociales elijen enmascarar sus identidades reales de diferentes formas. Algunos pueden hacerlo a través de un anonimato total, siempre que no sea necesario ningún nombre en absoluto para la utilización del servicio mientras que otros utilizan seudónimos de forma de ocultar su identidad real.

Estas opciones son un derecho que deben tener los usuarios, una opción que debería ser permitida. Algunas personas que pueden preferir un personaje anónimo o seudónimo pueden sentir la necesidad de una mayor privacidad, tener posturas u opiniones controvertidas, por los entornos laborales, incluso hasta vivir en un país con un gobierno autoritario. Podemos pensar en personas con condiciones médicas particulares o delicadas que deseen hablar sobre los síntomas y el tratamiento que están llevando sin necesidad de crear un registro público de su condición, bloggers y activistas de participación política especialmente en temas polémicos, víctimas de acoso, asalto sexual y violencia doméstica, etc.

Al iniciarse en una red social las personas pueden tener dudas sobre utilizar su identidad real, un seudónimo o permanecer anónimos en la red. La privacidad es una de las cuestiones más preocupantes que afecta al conjunto de los usuarios. Muchas han sido las protestas e incluso las demandas interpuestas a grandes compañías por violar el derecho a la privacidad de sus clientes. Actualmente existen dos modelos para que un usuario se muestre y actúe en Internet, basados en dos conceptos duales, el que defiende Facebook y en contraposición el de 4chan. Así como lo proponen y presentan sus respectivos creadores, haciendo una comparación entre los modelos de Marck Zuckerberg (creador de Facebook) y Christopher 'Moot' Poole (creador de 4chan), de la transparencia frente al anonimato, podemos observar grandes diferencias y las implicancias de cada uno. Según Zuckerberg, promocionar la propia identidad refuerza a la persona y previene

malas prácticas en Internet. En contraposición, Poole defiende la libertad de expresión en su máximo grado y cree que para eso el anonimato es la mejor opción y que esto favorece la creatividad.

De hecho, el anonimato es una herramienta útil para cualquier persona que prefiera mantener una clara separación entre su identidad fuera de línea y su identidad en línea. Las redes sociales mayormente no permiten un anonimato total, dado que esto va contra la naturaleza de estos servicios. Normalmente, aquellos usuarios que prefieren participar en redes sociales sin revelar su verdadera identidad crean perfiles utilizando un nombre falso o un seudónimo. Personalmente no suelo utilizarlos pero muchos usuarios si lo hacen, o simplemente son conocidos por estos seudónimos de tal forma que no los conocerías por sus nombres reales.

Es importante tener en cuenta la dificultad que implica mantener completamente independientes las dos identidades. Es posible divulgar información que las vincule a través de actualizaciones de estado, por otros miembros en algún grupo del que formemos parte, fotografías, redes de amigos y otros indicadores. De hecho, numerosos estudios han demostrado que los datos anónimos a menudo se pueden vincular a determinadas personas sin una complejidad relativamente importante.

Si pensamos utilizar un perfil bajo un seudónimo, es muy importante leer los términos del servicio para la rede social en cuestión. Proporcionar información falsa o incompleta viola los términos de algunos de estos sitios (existen excepciones

evidentemente, si no me pregunto que ocurre con los nombres de los artistas por ejemplo, si son tomados como reales o se están violando los términos del servicio).

Ya lo mencionamos pero debe quedar claro que es necesario realizar la lectura de la política de privacidad antes de marcar "Acepto", algo que por más que es necesario muchas personas pasan por alto al unirse a una red social (yo diría que casi todos lo hacemos). Debemos comprender que podemos obtener una gran cantidad de información útil mediante la revisión de la política de privacidad antes de registrarnos, y sin lugar a dudas revisando los cambios a las mismas durante el tiempo que estemos activos en ella. En éstas se explica cómo la plataforma recogerá, almacenará y utilizará la información sobre las personas que visitan el sitio. Se puede aprender mucho en este documento del funcionamiento de una red social y qué van a hacer con nuestra información.

Cierta información que los usuarios proporcionamos al registrarnos resulta muy evidente, como la fecha de nacimiento, pero muchas otras veces la red social recopila información sobre nosotros de forma invisible, mediante el seguimiento de cada acción individual que hacemos con nuestros perfiles de usuario, por ejemplo en qué enlaces se hace click e incluso los sitios web que se visitan después de salir de la red social.

Al revisar una política de privacidad debemos tener en cuenta que es una versión del documento en este momento, la imagen al día de hoy, pero que esas reglas pueden y van a cambiar, a veces se

dan cambios sustanciales tiempo después de que un usuario haya creado su cuenta, por lo que debemos estar atentos a los mismos. Existen sitios que revisan periódicamente las políticas de privacidad de las distintas redes sociales y mantienen un sistema de información para mantenernos actualizados, como es el caso de tosback.org que chequea estos documentos en más de 50 redes sociales.

Los términos del servicio es otro documento que debe ser leído en algún momento, contiene información tan importante como la política de privacidad. De cualquier manera debemos comprender que ambos documentos afectan solamente las actuaciones de esa red social y a los servicios que esta da por si misma, y no compromete de ninguna manera a ser responsable por ejemplo de cubrir las acciones que realicen las aplicaciones de terceros que interactúan con ella o las empresas que las desarrollan.

Desafortunadamente, la mayoría de estos documentos son extremadamente largos y difíciles de entender para el común de los usuarios, lo que sin duda dificulta la tarea. Veamos algunos puntos a considerar cuando se lee una política de privacidad de modo de hacer más sencilla su comprensión.

Un consejo rápido podría ser el de comenzar la lectura por el final del documento, la sección más importante de una política de privacidad suele ubicarse allí. Por ejemplo, un final del documento típico proporciona información de contacto privado de la empresa, así como los hechos más importantes acerca de cómo la información de identificación personal es utilizada. Así que,

cuando no tenga mucho tiempo, comience mirando el final del documento para hacerse de datos importantes como el de la forma de contactar con la red social ante eventualidades.

Si el tiempo del que disponemos para dedicarle a esta lectura es el suficiente, entonces debemos identificar la ubicación y el idioma de la política de privacidad dentro de la red social. ¿Está escondida? ¿Es difícil de encontrar en el sitio web o puede ser encontrada fácilmente? ¿El lenguaje utilizado parece demasiado vago o incomprensible? Estas variaciones pueden demostrar la intencionalidad del sitio en este aspecto, intentando facilitarnos la vida o todo lo contrario.

También se recomienda buscar la información referente a la cancelación de la cuenta. Si usted decide salir de la red social, ¿puede eliminar la cuenta y eliminar toda su información? ¿Todos los datos se eliminarán por completo o cierta información se mantendrá almacenada en esta red? Es importante entender qué es lo que sucederá con la información, fotos, etc. que hemos subido a la red durante el tiempo de uso al momento de eliminar el usuario.

¿Durante cuánto tiempo es almacenada la información personal? Tenga en cuenta que algunos datos pueden ser anónimos después de un cierto período de tiempo, algunos se pueden eliminar por completo y otros pueden ser almacenados perpetuamente por la red social. Debemos encontrar las reglas que expliquen lo qué sucede con la información cuando un

usuario muere ¿La política de privacidad explicita esta situación? ¿La cuenta se mantendrá en línea o se dará de baja?

Otra cuestión a tener en cuenta es a quién le pertenecen los datos que un usuario publica. Es necesario conocer como se maneja la propiedad intelectual de las fotos y videos, por ejemplo. ¿Un usuario puede perder el derecho a la información que él o ella publica? ¿La misma puede ser utilizada por el área de mercadeo sin el consentimiento expreso del usuario? Por ejemplo, ¿puede utilizarse el nombre de usuario y sus fotos para anuncios publicitarios? ¿Quién tiene acceso a la información además de la red social y mis contactos?

También debemos saber como realizar una queja. Es necesario contar con una dirección física, de correo electrónico, la dirección del sitio web o un número de teléfono donde los usuarios puedan expresar sus inquietudes respecto a la privacidad. Algunas redes sociales utilizan empresas independientes que revisan sus prácticas de privacidad, en tales casos los usuarios que no están satisfechos con el cumplimiento de la política de privacidad pueden presentar reclamos a la empresa certificadora.

Más allá de los servicios como el de Tosback, es importante conocer la forma en que los cambios en las políticas de privacidad son comunicados a los usuarios. ¿Estos se publicarán en la página de inicio o sólo se publicarán en la política de privacidad en sí misma? ¿Pueden los usuarios conectarse con un perfil público dentro de la propia red social que les mantenga informados de los

cambios en la política de privacidad u otros documentos? ¿Existe una forma de recibir un correo electrónico si se realizan cambios?

Resulta interesante leer lo que otros usuarios dicen acerca de la política de un determinado sitio. Una simple búsqueda en Internet podría significar un análisis profundo de la misma, especialmente para aquellas redes sociales que son de gran tráfico.

Con el fin de abordar las preocupaciones de sus usuarios con respecto a la privacidad, muchas redes sociales les permiten ocultar sus perfiles personales al público en general con distintas configuraciones de privacidad. Incluso en estos casos es posible inferir información personal que un usuario no desea hacer pública a través de distintos análisis. Un trabajo presentado en la Universidad de Maryland muestra cómo alguien interesado en recopilar información puede explotar una red social en línea con una mezcla de perfiles de usuarios públicos y privados para predecir los atributos personales de éstos. Los autores ubican este problema como de “clasificación de relación” y por lo tanto, se proponen modelos prácticos que utilizan la amistad y la información de pertenencia a grupos (que no son generalmente ocultos) para deducir los atributos sensibles de los distintos usuarios. La novedad en este estudio es la de incluir además de lazos de amistad los grupos, que pueden ser portadores de información significativa.

Lograron demostrar que en varios sitios sociales bien conocidos (el trabajo analiza entre otros a Flickr y Facebook) es posible fácilmente y con un nivel de exactitud importante, recuperar la

información privada de los perfiles de los usuarios. Por ejemplo se intentó predecir el género (sexo) del usuario y su filiación política, utilizando tres tipos de ataques: mixtos, sólo por enlaces de amistad, o por grupos de pertenencia. El resultado alcanzado fue de un 77% de acierto en género y un 58% de acierto en filiación política.

Mientras que tener un perfil privado es una buena medida para los usuarios preocupados por la privacidad, los vínculos con otras personas y afiliaciones con entidades públicas plantean una amenaza a la misma y dejan un hueco por el cual poder acceder a ella, porque como veremos más adelante, su seguridad depende en gran medida de la seguridad de sus amigos o contactos.

Se distinguió que es posible explotar una red social con perfiles mixtos entre privados y públicos para predecir las cualidades sensibles de los usuarios. Al utilizar información de los grupos de pertenencia, los atributos personales de algunos usuarios han sido descubiertos con una precisión sorprendente.

La privacidad en Facebook y otras redes sociales es tema de atención constante. Hace un tiempo lo que comenzó siendo apenas un proyecto presentado por dos estudiantes del MIT, hizo surgir grandes preocupaciones sobre cuánta información personal revelamos en la red aún sin ser conscientes de hacerlo, y de cómo esta puede ser utilizada por terceros. Esto que se dio a conocer en el mundo a través del periódico Boston Globe a través de un artículo en 2009 sobre la privacidad en línea titulado “Proyecto Gaydar”, se reveló la existencia de un software que

básicamente busca en la lista de amigos que un usuario posee en Facebook y mediante esta información puede determinar con cierta precisión si el usuario es homosexual o no. El programa simplemente contempla el género y la sexualidad de los amigos de una persona y mediante el análisis estadístico de estos hace una predicción.

Sin entrar en cuestiones de clasificación de un individuo por cualquier característica y problemas de discriminación, el asunto que nos interesa aquí es la facilidad con la que recorriendo la lista de amigos se puede obtener información sensible sobre el usuario.

Otro estudio realizado en la Universidad de Texas llamado "Inferring Private Information Using Social Network Data" basándose en el hecho de que los usuarios cada vez utilizan más las redes sociales y comparten en ellas todo tipo de información personal, concluye que cualquier organización, utilizando diferentes algoritmos, puede preveer o inferir información personal no divulgada directamente por el usuario, dejando de manifiesto que el problema de la protección de la privacidad en línea en redes sociales es algo muy real. Este trabajo muestra la predicción de las afiliaciones políticas como un ejemplo de esta realidad. Se estudiaron unos 167.000 perfiles y 3 millones de enlaces de personas ubicadas geográficamente en Dallas-Fort Worth en los Estados Unidos, mediante la creación de un crawler o robot que recorre Facebook y almacena la información necesaria para el posterior análisis. Se utilizaron tres métodos

para predecir las opiniones políticas de una persona: un modelo de predicción utilizando solamente los detalles en sus perfiles, otro utilizando enlaces de amistad, y el tercero combinando los dos conjuntos de datos. Los investigadores encontraron que ciertos rasgos, como saber qué personas o grupos conformaban la música favorita de un usuario, eran bastante predictivos de su afiliación política. Los mejores resultados, como en otros estudios, se dieron en la combinación de los dos enfoques. El estudio también especifica cómo poner en marcha ataques de inferencia utilizando datos publicados en redes sociales para predecir la información privada de las personas, así como la eficacia de posibles técnicas que pueden utilizarse para combatir este tipo de ataques a nuestra información, abordando diversas cuestiones relacionadas con las fugas de información privada en las redes sociales y explorando el efecto de eliminar los rasgos y los enlaces en la prevención de fugas de información sensible.

Los resultados indicaron que la eliminación de los rasgos detallados y los lazos de amistad en conjunto es la mejor manera de reducir la precisión del clasificador, pero esto se torna inviable en el mantenimiento de la utilización de las redes sociales, dado que estas medidas atentan contra la naturaleza de estos sitios. Sin embargo, también muestra que sólo mediante la eliminación de los rasgos del usuario de la información pública, se reduce en gran medida la precisión en la estimación de esta información.

Ahora estamos presenciando un nuevo escenario, la utilización de las redes sociales por parte de la policía. En particular y como

ejemplo el departamento de policía de Nueva York ha formado una unidad específica para vigilar las redes de comunicación social, dando un nuevo paso en el uso de la información pública ubicada en redes sociales para combatir la criminalidad. El objetivo es atrapar a los criminales que usan Facebook y Twitter principalmente anunciando sus planes para violar la ley o alardeando de los crímenes cometidos.

En junio de 2011, una fiesta en el este de Nueva York, más precisamente en Brooklyn, anunciada en Facebook como "Freaky Friday", terminó en un tiroteo que dejó un muerto y siete heridos. Después de ese incidente el comisionado de Policía Ray Kelly dijo a los periodistas "Nos fijamos en las redes sociales. Estamos muy centrados en estos festejos, como el que sucedió la semana pasada, y los visitamos antes de tiempo. Sin embargo, no todas estas fiestas ocurren en un lugar que se puede detectar con facilidad, muchas de estas cosas suceden en los apartamentos de la gente." Por otro lado en marzo de 2011, un joven de 18 años de edad, Anthony Collao fue asesinado en un ataque anti-gay en Woodhaven, Queens. El lugar de la reunión había sido anunciado en Facebook. Calvin Pietri, uno de los seis detenidos por el crimen, se jactó de la muerte en Facebook.

Como todo en la vida las opiniones son dispares, en una encuesta realizada a ciudadanos de Nueva York sobre lo que pensaban de policías husmeando en Facebook y Twitter se obtuvieron diferentes resultados. Mientras unos decían "si va a ayudar a reducir los homicidios, entonces supongo que estoy a favor de

ello", otras personas se lamentaban diciendo "yo realmente creo que es una invasión de la privacidad."

De esta forma, los policías de Nueva York seleccionados para trabajar en el nuevo grupo tienen como objetivo rastrear las redes sociales para estar informados sobre los movimientos en la web, de forma de poder anticiparse a concentraciones masivas o planes que puedan desencadenar situaciones violentas. Estas actividades van en aumento en muchas partes del mundo basados en la lucha contra la criminalidad pero con una preocupante posible intromisión en la privacidad de los usuarios en las redes sociales.

La relación entre el caos y los medios de comunicación social se pusieron sobre la mesa con las concentraciones y actos masivos que derivaron en incidentes en Inglaterra. Éstas se organizaron, o mejor dicho se potenciaron con la difusión a través de Twitter y los mensajes de Blackberry. Esta situación hizo reflexionar a los gobiernos y a los cuerpos policiales en varias partes del mundo. Las redes sociales fueron muy criticadas y acusadas de ser el motor para coordinar los disturbios. El servicio de Blackberry Messenger ha sido citado por muchos como la herramienta de comunicación más utilizada por los participantes en los disturbios en Inglaterra. Las medidas tomadas por el Gobierno y la Policía en esos incidentes también han marcado una realidad.

4. LA RED TIENE MEMORIA DE ELEFANTE.

Todos o casi todos hemos oído alguna vez las frases “un elefante nunca olvida” o “tiene memoria de elefante”, aludiendo o remarcado la memoria de largo plazo como una cualidad de destaque. Bueno, la realidad es que en Internet es donde realmente nunca se olvida, donde reside esa memoria de elefante, con la capacidad de a largo plazo recordarlo todo.

La red cuenta con zettabytes de capacidad de almacenamiento donde se puede guardar todo, es posible buscar y encontrar cualquier información en cuestión de segundos gracias a motores de búsqueda como Google, Bing o Yahoo; de tal forma de que podemos pensar como imposible el eliminar por completo la información cargada alguna vez en la red.

Si bien no es recomendable cambiar su identidad para tratar de esquivar su pasado digital (aunque algunas veces parezca la única solución), si recomiendo enormemente que ejercite un mínimo de discreción y sentido común respecto a la información que publica en línea.

El auge sin precedentes que han tenido el voyeurismo por un lado, y el exhibicionismo por otro, han modificado lo que antiguamente conocíamos como “contar chismes”. La gente no está distinguiendo la intimidad de la extimidad (entendamos por

extimidad la necesidad de las personas de externalizar la intimidad) y este aspecto ha adquirido mayor relevancia con el auge de las redes sociales.

Con la llegada de Internet hay personas que prefieren contar su vida en línea antes que a un familiar. El problema, que si bien es una realidad conocida desde siempre está tomando un cariz importante, es que el ser humano necesita privacidad pero al mismo tiempo publicidad. Lo que podemos observar es que ahora más que nunca parece estar pesando en esta ecuación mucho más lo segundo que lo primero.

Llegará el día en que queramos escapar de nuestro pasado digital, escondernos de nosotros mismos, olvidar lo que una vez dijimos o hicimos, pero esto estará almacenado en algún servidor, escondido y protegido por millones de hiperenlaces. Como dijo Eric Schmidt en agosto de 2010, demasiada información será compartida en línea, y la gente un día cambiará su nombre y se reinventará a sí misma con el fin de escapar de su pasado digital. Una vez que algo es publicado se puede compartir en cuestión de segundos en el mundo entero, y permanecerá allí por décadas y en algunos sitios por siempre.

En la red todo queda grabado, notas, fotos, videos, comentarios de terceros. Atravesamos una época de grabación permanente de la memoria colectiva. Los casos como ejemplos de esta realidad se repiten en todo el mundo. Podemos pensar como algo lógico el que una pareja de la vida real sean amigos en Facebook, que digan que son pareja y que compartan información en el

Twitterverse (universo de Twitter). Hasta que la relación termina. A partir de ese momento desean cortar todos los vínculos y eliminar todas las cosas que han dicho en línea. Según se publico en una historia del NYTimes un profesor de Nueva York recientemente divorciado de su esposa tras cinco años de matrimonio al hacer una simple búsqueda ingresando su nombre en Google seguían encontrando fotos de las vacaciones de él y su ex mujer, así como las fiestas de Navidad. “Es difícil conseguir una nueva cita cuando al hacer una simple búsqueda en la web sigues estando presente junto a tu ex”, razonaba este individuo. Lo mismo sucede con informes de prensa, acusaciones falsas (o no), multas u otro tipo de infracción que se publique en la web; allí están y allí quedarán por siempre.

Ni hablar de comentarios políticos, aunque sus ideas cambien con el tiempo, ese comentario o artículo publicado jamás lo hará, al igual que comentarios ofensivos suyos o en su contra, fotos que evidencien una noche de borrachera o cualquier otro tipo de contenido que pueda en algún momento ser comprometedor.

El hecho de que la web no olvida da lugar al debate de si estamos ante el adiós a las segundas oportunidades en la vida de las personas. Viktor Mayer-Schönberger, profesor de Reglamentos y Gobernabilidad de Internet en el Oxford Internet Institute de la Universidad de Oxford, está promoviendo una discusión sobre este tema basándose en su libro “Delete - La virtud de olvidar en la era digital”. En el mismo sostiene que durante milenios lo difícil fue recordar, y lo fácil olvidar.

Hasta ahora los soportes necesarios en los cuales almacenar y conservar la información eran costosos, la búsqueda se hacía difícil y el acceso era muy limitado, por lo cual era lógico que sólo permaneciera lo esencial. Pero en esta era digital, el almacenamiento de datos no sólo es mucho más sencillo sino que mucho más barato, lo que lo hace casi ilimitado, con un crecimiento en la red de los servicios de almacenamiento que ha sido explosivo con la computación en nube: ya casi nada se elimina, todo se almacena.

El libro comienza contando lo acontecido a Stacy Snayder una joven de 25 años que al finalizar sus estudios para ser maestra le fue negado su diploma. La justificación de la Universidad fue el comportamiento poco profesional que demostraba Stacy en una fotografía que había subido a su página en MySpace, bebiendo alcohol y disfrazada de pirata, a la que tituló “La Pirata Borracha”. Más allá de la estupidez mostrada en la decisión de la Universidad, el problema dice el autor es la importancia de olvidar, y la incapacidad de hacerlo que presenta la red. Anteriormente, la sociedad aceptaba que los seres humanos evolucionábamos a medida que transcurría el tiempo y que aprendíamos de las experiencias pasadas, ajustando así nuestro comportamiento, pero en una sociedad en la que todo queda grabado, no podemos en la práctica escapar de nuestro pasado. La opción por defecto es la de conservar y memorizar toda la información.

Quizás los problemas de Stacy fueron ocasionados por ella misma, al subir una foto que podía comprometerla, con una descripción no muy feliz y sin pensar que esta iba a ser accedida por todos, y recordada aún mucho tiempo después de que hubiese ocurrido. La incógnita que se presenta ahora es saber cómo se comportarán los nativos digitales dentro de 20 años. Quizás las generaciones siguientes reaccionen de forma distinta, atribuyan al contenido colgado en Internet un valor diferente y retomen el camino de que el tiempo modifica nuestro comportamiento porque de todo se aprende algo: por ejemplo, que consideren un mail incauto o una foto comprometedora o una crítica gratuita en un foro de tiempo atrás como poco relevante para el momento actual.

En una primera instancia algunos usuarios con este tipo de problemas intentaron manipular los resultados de las búsquedas web por su cuenta, en una acción desesperada por sacar de los primeros resultados de búsqueda aquellos contenidos que eran negativos para ellos, haciendo cosas como el eliminar manualmente las fotos de Flickr, cambiando niveles de privacidad, haciendo revisiones de las páginas de Facebook y pidiendo a los bloggers que eliminasen los mensajes ofensivos, entre otras cosas. Pero al igual que un cáncer, los datos negativos, la información que no querían que se viera, ya se ha incrustado en lo más profundo del ciberespacio, grabado en los archivos, los algoritmos y está protegido por una red de hiperenlaces; y por más que se quiera e intente extirpar completamente, esto resulta imposible.

Al no poder deshacerse de los contenidos negativos por sí mismos, muchos de estos usuarios dirigieron su atención a un grupo de especialistas en la web conocidos como gestores de la reputación online, que ofrecen borrar los mensajes negativos, enterrar los resultados desfavorables de búsqueda y hacer un seguimiento de la imagen en la red de sus clientes. De esta forma al realizar una búsqueda en Internet de sí mismos, resulta que los enlaces a contenidos negativos o perjudiciales son más difíciles de encontrar, dado que han sido enterrados en los resultados orgánicos de los buscadores web luego de seis o siete páginas. Debemos dejar en claro que si bien seguirán estando accesibles y no serán olvidados por la red, lo que estas personas hacen es que los contenidos sean más difíciles de encontrar al navegar la web.

Una de estas empresas es Reputation.com, gestores de la reputación online que prometen hacer que sus clientes se vean mejor en la red. Más adelante hablaremos de este tema en profundidad, pero en una época en que la reputación de una persona es cada vez más definida por parte de Google, Facebook y Twitter, estos sitios ofrecen servicios que esencialmente manejan un cambio de la imagen en línea, mejorando la forma en que alguien aparece en Internet, por lo general poniendo de relieve las características positivas y ocultando las negativas.

Michael Fertik, director ejecutivo de Reputation.com sostiene que Internet se ha convertido en el recurso go-to para destruir la vida en línea de alguien, que a su vez impacta en forma significativa en su vida fuera de línea. Estos servicios de imagen en línea no

son totalmente nuevos, desde hace años las grandes corporaciones y otras empresas con intereses financieros en su presencia en la Web han empleado técnicos para editar su reputación en ella, servicios que generalmente les son ofrecidos como parte de un paquete de gestión web de alguna gran empresa de relaciones públicas o asesores de imagen.

Por ejemplo, durante el colapso económico en 2008, algunos banqueros de Wall Street contrataron especialistas de Internet para proteger su buen nombre, o algo así. Algunos estaban pagando más de diez mil dólares por mes para tratar de ocultar sus nombres en la red, ya que habían comenzado a aparecer en la prensa. Las personas famosas del mundo del espectáculo también han utilizado a estas empresas para defenderse de chismes que les perjudican, o artículos negativos en los diferentes medios de comunicación.

Ya no es aceptable realizar denuncias y juicios con liviandad, sobre todo después del incidente de Bárbara Streisand con las fotos tomadas de la costa de California donde se veía su casa. La cantante había demandado hace unos años al fotógrafo Kenneth Adelman y la página de fotografías Pictopia.com al tomar fotos de la costa de California y publicarlas en su web, donde se veía la casa de Streisand. Aludiendo a su derecho a la privacidad, lo que consiguió fue dar a conocer su casa en todo el mundo, ganó la demanda y el juez emitió una orden para que la fotografía en cuestión fuese retirada del sitio. Claro que lo que sucedió verdaderamente dista mucho del objetivo buscado, mientras esta

resolución judicial ocurría el tema se propagó por la web como reguero de pólvora y la foto fue compartida en muchísimos otros sitios y páginas, se volvió el comentario de la red, incluso aún hoy la foto está visible en varios sitios. Algo que pudo pasar inadvertido fue potenciado por la intención de sacarlo del aire. Desde entonces cada vez que alguien intenta vetar algún contenido en la red los cibernautas reaccionan en lo que se conoce como “el efecto Streisand”. Para ser más claros, como se define esto en Wikipedia se define de forma sencilla: “se denomina El efecto Streisand a un fenómeno de Internet en el que un intento de censura u ocultamiento de cierta información fracasa o es incluso contraproducente para el censor, ya que ésta acaba siendo ampliamente divulgada, recibiendo mayor publicidad de la que habría tenido si no se la hubiese pretendido acallar.” Y como la red no olvida, la foto está visible en varios blogs, sitios, almacenada, y recordada por siempre, sin importar lo que un juez dictaminó.

Como la gente común comenzó a vivir más tiempo de sus vidas en línea, ya sea escribiendo un blog sobre la cena o publicando fotos de las vacaciones en Facebook, el sobreexponer la información comenzó a ser un tema del día a día. Esto, que veremos más adelante, trajo aparejado un crecimiento muy importante en la cantidad de información del círculo de intimidad de las personas en un proceso de extimidad acelerado. Dentro del manejo de estos contenidos para tratar de administrar la reputación se dividen a las personas en dos tipos: los reactivos que quieren eliminar un elemento específico de la Web, y aquellos

usuarios proactivos que quieren controlar su imagen. Se puede ver dentro de estos grupos de individuos desde personas famosas, estudiantes universitarios tratando de eliminar las fotos en fiestas y borracheras o simplemente fotos comprometedoras antes que los reclutadores corporativos los encuentren, hasta profesionales que pretenden eliminar fotos de sí mismos no relacionadas con el trabajo mientras tratan de obtener un ascenso. Esta cantidad de información que ahora pertenece a la extimidad ha quedado almacenada en la red.

Una pregunta que muchos nos hemos hecho alguna vez es ¿por qué tiene tanto peso en la mente humana la información perjudicial? Es algo conocido que los seres humanos nos acordamos más de las cosas negativas que de las positivas, de lo malo que de lo bueno o simplemente que lo perjudicial tiene preponderancia; la sencilla razón es esencialmente de psicología evolutiva: por ejemplo, si no recordáramos que esta agua está contaminada, entonces al beberla podríamos no sobrevivir; en cambio, si nos olvidamos algo positivo como que esta agua es muy fresca y bebible, la consecuencia es menos grave que lo anterior, simplemente lo que sucede es una pérdida en términos de oportunidad, en este caso de beber agua fresca.

Pero además de este concepto evolutivo, la información negativa resiste al paso de los años con mayor facilidad que la positiva, e influye en el juicio y las apreciaciones de las personas. En cambio, los aspectos buenos, cuando son antiguos, apenas compensan los malos. Para quien ganó un premio hace tres meses esto tendrá

un impacto positivo para su reputación, pero si el premio se remonta a más de tres años el efecto será residual. Sin embargo un hecho negativo es más potente, su duración y su impacto a lo largo del tiempo son mayores, quedando en la mente e influyendo en la opinión de los demás hacia nosotros. Eventos como ser detenido ebrio mientras se conduce serán difíciles de olvidar por la red, y a ella tampoco le importará exactamente cuándo ocurrió, allí estará la información almacenada, disponible y de fácil acceso para todos cuando lo deseen.

La información que es contraproducente para nuestra persona tiene una ventaja añadida en Internet, la velocidad de propagación de la crítica es muy superior a la del elogio. Un solo comentario de volverse viral puede hundir la reputación de un usuario al conseguir encabezar las páginas de resultados de un motor de búsqueda como Google. Esto es como esa vieja frase que desde chicos vemos en almacenes u hoteles “un cliente insatisfecho habla con 11 personas y uno satisfecho con 2 ó 3”. Aunque se consiga eliminar o apaciguar el impacto de un contenido negativo en la red, siempre quedarán los restos de la batalla, al igual que una cicatriz.

Como ya lo mencionáramos, una vez que algo está en línea será muy difícil eliminarlo, por lo que las posibilidades generalmente se reducen a jugar con los motores de búsqueda. Personas pendientes de su imagen en línea y con algún conocimiento de la Web y su funcionamiento pueden tratar de hacerlo por si mismos, al llenar Internet con contenidos favorables. Esto podría incluir la

creación de su propio sitio web o blog, a la suscripción a las redes sociales más populares como Facebook, Twitter y LinkedIn. Con un poco de suerte, estos sitios van a aparecer primeros en una búsqueda en Internet, y de esta forma presionen hacia abajo cualquier material ofensivo. Pero estas tácticas tienen sus límites, especialmente cuando los contenidos en cuestión están publicados en sitios web populares y optimizados para los motores de búsqueda.

El sitio web Gawker, un blog de medios de comunicación de Nueva York, publicó una serie de artículos sarcásticos sobre Julia Allison, una ex-columnista de la revista Time Out de la misma ciudad y experta en medios de comunicación social, en los que incluyeron correos electrónicos y fotos de esta persona en ropa interior. Ella intentó hacer modificaciones por su cuenta y luego acudió a una empresa para que interviniera en estos temas y lograra evitar esos contenidos.

Al final la Sra. Allison compara la cicatriz de su reputación en línea a un gran tatuaje "Técnicamente, es posible eliminarla, pero es doloroso y costoso. Además, no hay garantía de que puedas eliminar el 100 por ciento del problema". Toda esta experiencia la ha hecho más cauta acerca de lo que ella comparte en línea. Si bien aún hay unas pocas fotos en lencería, las que ahora desea que sean privadas, considera que son las equivocaciones promedio de la juventud, y comentó "Por desgracia, son errores que ahora me van a seguir de forma permanente."

Insafe, una organización europea de la cual forma parte la Unión Europea como co-fundadora, se dedica a promover la seguridad y la responsabilidad en el uso de Internet y los dispositivos móviles por parte de los jóvenes y tiene como misión como dice su propio sitio web “Capacitar a los ciudadanos en el uso de Internet, así como otras tecnologías en línea, de manera positiva, segura y eficaz”. La red exige la responsabilidad compartida en la protección de los derechos y necesidades de los ciudadanos, en particular los niños y jóvenes, por parte del gobierno, educadores, padres, medios de comunicación, la industria y todos los demás interesados. Los asociados en Insafe buscan generar en los usuarios de Internet la idea acerca de que algunos contenidos pueden ser nocivos o hasta ilegales, mediante una estrecha cooperación entre distintos actores, pretendiendo de esta manera aumentar la conciencia individual y colectiva sobre la seguridad en Internet.

Esta organización lanzó una campaña llamada ThinkB4Upost “piensa antes de publicar”, para sensibilizar a los más jóvenes sobre los peligros de la memoria de Internet, sobre todo si algunas imágenes están sacadas de contexto. “Una vez que cuelgas tu foto, no la puedes retirar; todos la pueden ver: amigos, familia, cualquiera”, reza el lema de la campaña. Esta se puede ver en el sitio web de Insafe o mismo en Youtube, es muy sencilla con un mensaje diáfano, “piense antes de actuar”.

5. LA REPUTACIÓN 'ONLINE'.

Si bien este es un tema que ya veníamos tratando en el capítulo anterior, veremos algo más en detalle. La gestión de la reputación online es una necesidad creciente cada día, sin embargo la mayoría de los individuos y las organizaciones siguen manteniendo su presencia online sin asumir una estrategia de gestión de la misma, lo que en algún momento puede generar consecuencias negativas para ellas.

Cada cosa que hacemos en la red así como cada contenido que publicamos, ya sea una foto, un video, un tweet, un post o un simple comentario en un blog; contribuye a construir, configurar y reforzar nuestro branding personal o el de nuestra empresa según sea el caso. En Internet no sólo las empresas sino todos y cada uno de nosotros somos nuestra propia marca, pero ahora nos estamos dedicando a la presencia de un individuo, por eso hablaremos de branding y reputación personal y no de estrategias para empresas.

Es importante que los usuarios piensen o reflexionen antes de lanzarse o cuando van a realizar una acción en la red, y sobre todo en las redes sociales: definir o conocer qué es lo que deseamos transmitir en el medio online, nuestros valores, estilo de vida, nuestra imagen, etc. y si lo que subimos a la red se condice con esto.

El actuar sin pensar es posiblemente el primer y más grave error, confundir a nuestra audiencia, generar dudas fundadas sobre nuestra credibilidad y nuestra personalidad puede traer consecuencias negativas. Se sabe que el 70% de los reclutadores en Estados Unidos ha rechazado candidatos basados en esta información ubicada en Internet. Esto ha creado la necesidad de controlar varios aspectos de la privacidad en las redes sociales en adición a controlar tu reputación online.

La capacidad para hacer consultas en línea acerca de las personas ha crecido dramáticamente en los últimos años, así como la cantidad de información que compartimos en las redes sociales. Por ejemplo al comenzar el 2012, Facebook tiene unos 850 millones de usuarios y en su plataforma se manejan 2.700 millones de actualizaciones y "me gusta" cada día. Twitter por otro lado, está en los 500 millones de usuarios registrados y se postean en su red unos 290 millones de tweets por día.

Algunas empresas están ganando dinero, vendiendo servicios para hacer investigaciones en todas las redes sociales, búsqueda de información en particular de diferentes personas. Estos servicios son contratados por empresas y/o reclutadores: "esto puede ayudar a la contratación de personal", argumentan los profesionales dedicados a estas tareas. Esta investigación o búsqueda de información es usada en la toma de decisión al momento de contratar o no a un individuo. El aparecer a veces borracho en una fiesta, o fumando marihuana o habiendo escrito una broma que puede ser interpretada como un posible prejuicio

racial o discriminatorio influyen negativamente en una valoración que nos hará menos deseados a la hora de elegir a quién contratar, por lo que no es extraño que se maneje por parte de algunas personas un concepto denominado “el costo de comportarse como un idiota en Internet”. Como las redes sociales tienen relativamente poco tiempo de existencia y la maduración en su uso no es la suficiente, muchas personas se comportan como verdaderos idiotas, exponiendo su vida privada o situaciones comprometedoras al escrutinio público. Podemos pensar, y quizás con cierta razón, que la vida personal no debería influir en una empresa al punto de decidir una contratación, pero el hecho es que las redes sociales se están convirtiendo en uno de los criterios de filtro para los nuevos reclutadores, e incluso afectan la oportunidad de acceder a ascensos en el propio trabajo. Lo más extraño, es que a la gente parece no importarle demasiado esta realidad.

Un tema delicado a tener en cuenta dentro de la gestión de nuestra reputación es la monitorización de la presencia en la Web y las redes sociales, no sólo para poder analizar y evaluar nuestras acciones, sino también para conocer el impacto de éstas y la valoración que estamos teniendo. Para poder reaccionar, de ser necesario con la celeridad adecuada ante situaciones potencialmente dañinas para nuestra reputación, así como para poder aprovechar situaciones potencialmente positivas y capitalizarlas en nuestro favor, existen distintas herramientas monitoreo, algunas pagas y otras que son sin costo y que se ajustan según las necesidades de cada caso.

De todas formas, antes de generar algún contenido, debemos reflexionar acerca del público objetivo, el tipo de información que estamos publicando, el tono de la misma, y principalmente si ese contenido, ya sea una imagen, un post, un video o simplemente una actualización de estado, serán positivos o negativos para el manejo de nuestra reputación. Por ejemplo, es necesario pensar unos segundos antes de escribir un tweet y volver a pensar otros segundos antes de actualizarlo en la red.

Sin respuestas acertadas en estos temas o con ideas equivocadas, nos exponemos a generar contenidos que puedan desatar crisis de reputación o que influyan negativamente sobre ésta. Lógicamente debemos prestar atención a la respuesta obtenida y permanecer flexibles para variar el rumbo de ser necesario, o dar preferencia a ciertos canales sobre otros (imágenes, videos, comentarios, etc.) para determinados tipos de contenidos.

Cada día hay más personas que piensan: “hay momentos en los que solo hay que contarle a tus amigos acerca de algo, pero no necesariamente a tus amigos de Facebook”. La política que la mayoría de las personas tiene en la red social sobre los “amigos” en el mejor de los casos lo limita a “conocidos”, personas con las que alguna vez tuvieron trato o compartieron algo. La facilidad con la que las redes sociales permiten incorporar contactos a nuestros perfiles han conseguido que seamos más sociables estando en línea que en el mundo real.

Un estudio realizado en el Reino Unido por la fundación dedicada a combatir la fibrosis quística encontró que una persona tiene el doble de amigos en las redes sociales que en el mundo real y que tiende a ser más abierta, confiada y sincera con sus amigos virtuales que con los reales. Con estos datos sostiene que la vida en la red mejora la calidad de vida real de las personas con enfermedades, sobre todo aquellas que ven limitadas sus capacidades motrices. Otra encuesta realizada por la empresa de servicios de seguridad en Internet, HomeSafe TalkTalk, ha mostrado que los niños pasan un promedio de dos horas y seis minutos online al día. Se ha encontrado que el 50 por ciento de los adolescentes de edades entre 12 y 17 años utiliza las redes sociales "todos los días".

Los niños y jóvenes menores de 18 años nunca han conocido un mundo sin Internet. Los jóvenes de 24 años de edad comenzaron su educación primaria en un mundo en red, una distinta a la actual, pero red al fin.

Internet ha revolucionado la forma en que aprenden, juegan y se comunican entre sí. Estos jóvenes conocidos como nativos digitales tienen una percepción del mundo y sobre todo de la forma de relacionarse unos con otros, muy distinta a la de los arcaicos adultos mayores de 30 años de edad.

Surgen también cada vez más servicios que permiten a los usuarios de redes sociales subir y compartir imágenes, videos y hasta mensajes restringiendo mejor el grupo de individuos que acceden a estos contenidos, como es el caso de www.path.com

Path es un sitio web donde se puede compartir información con una red de 50 amigos cercanos, y no la vorágine de amigos o los conocidos de Facebook. Hay una diferencia entre las personas a las que considero mis amigos y aquellos que son conocidos, personas con las que he tenido algún tipo de relación pero que no integran mi núcleo más íntimo de amistad.

Otros sitios web sociales que ofrecen este tipo de servicios para evitar la sobreexposición son GroupMe, Frenzy, Rally Up, Shizzlr, Huddl y Bubbla.

Esta situación se ve reflejada en que los usuarios de Facebook están creando grupos de amigos con una media de 8 personas por grupo, según informa la propia red social, y que la red en sí ha modificado sus métodos de compartir información para poder restringir quienes ven lo que subimos a la red.

La reputación en los servicios de transacciones comerciales es otra situación a considerar, habida cuenta de la maleabilidad de las identidades en línea, algunos economistas habían expresado su sorpresa de que sitios de comercio electrónico como eBay se hayan desarrollado tan fuertemente en Internet. Cuando dos usuarios del servicio que representan dos identidades se proponen iniciar una transacción en línea se enfrentan con el dilema del prisionero, el acuerdo sólo puede tener éxito si las partes están dispuestas a confiar en el otro, pero carecen de una base racional para hacerlo.

Pero, para que estos sitios comerciales en Internet hayan tenido éxito han debido desarrollar sistemas de gestión de reputación internos a su plataforma; como el sistema de votos de eBay, donde se registran las operaciones y se proporcionan los medios técnicos para que los usuarios puedan valorar a otros usuarios con los que han realizado alguna transacción con puntos de confianza. El sistema se basa en la emisión de un voto sobre la transacción para reflejar la experiencia con el comprador o vendedor. Este voto se le solicita a ambas partes involucradas en cada transacción que se realiza allí.

Con este sistema los usuarios adquieren una reputación basada en los comentarios y en la puntuación otorgada por otros usuarios, reflejando la confianza que se puede tener en un comprador o vendedor potencial de un producto deseado.

Una vez escuché a alguien decir que "una persona será tan confiable en el mundo de los negocios como su puntuación o reputación en eBay". Exagerado o no, por lo menos en el mundo virtual esto no deja de ser una realidad, aquellos que han realizado transacciones en este sistema saben que el tener una buena reputación o el no tener una mala reputación es fundamental para realizar una transacción.

Otro tema interesante para la reputación online es el “scoring” o sistemas de puntuación de nuestra presencia en el mundo digital. Pensemos que en el mundo virtual se nos asigna un número que indica la influencia que tenemos, este número podría ayudar a determinar si nos aceptan en un trabajo, si nos mejoran la

habitación del hotel, nos dan muestras gratis en el supermercado o incluso el acceder a un lanzamiento de un nuevo servicio en Internet con anticipación. Si su puntaje de influencia es bajo, no consigue el ascenso, la suite o las galletas de cortesía. Bueno, esto no es ciencia ficción, es lo que está sucediendo con los usuarios de las redes sociales, incorporando los perfiles de Linkedin, Facebook, Twitter, Quora, etc. a servicios de scoring social.

Nuestras cuentas en esas redes ya están siendo juzgadas o analizadas por empresas como Klout, PeerIndex o Twitter Grader, que han desarrollado procesos y sistemas de puntuación que les permiten clasificar a millones de personas sobre su nivel de influencia. Estas no están simplemente observando el número de seguidores o amigos que han acumulado, están midiendo la influencia de una manera más matizada con la publicación de sus posts, tweets, o actualizaciones de estado en forma de una puntuación en línea, y continúan refinando sus métodos de evaluación a través de otros sitios de redes sociales día a día.

Esta puntuación es accesible públicamente por todo el mundo, incluso las personas con las que sales, o con las que trabajas a diario. Las puntuaciones de influencia suelen oscilar entre 1 y 100, en Klout, el sitio principal en este servicio (la puntuación media se encuentra en los adolescentes mayores). Una puntuación en el entorno de 40 sugiere una presencia fuerte, pero de nicho. Si tienes 100, por el contrario, significa que eres Justin Bieber. En PeerIndex, otro de los sitios con mayor auge, la

puntuación media es de 19. Un perfecto 100, según la compañía, significa que eres "como un dios".

El marketing está sumándose a esta idea con más de 2.500 empresas utilizando los datos de Klout. El sitio de scoring reveló que Audi podría comenzar a ofrecer promociones a los usuarios de Facebook basándose en su puntuación de Klout. A modo de ejemplo de algunas acciones concretas, Virgin America utilizó los datos de la empresa para ofrecer a personas influyentes con una alta calificación en Toronto vuelos gratis de ida y vuelta a San Francisco o Los Ángeles; en Las Vegas el Palms Hotel y Casino está utilizando datos Klout para ofrecer a los huéspedes de alta calificación una mejora en su habitación o boletos para el Cirque du Soleil.

Quienes defienden esta idea sostienen que se fomenta la democratización de la influencia; ya no tienes que ser una celebridad, un político o una personalidad de los medios para ser considerado influyente, la calificación social también puede ayudar a construir una marca personal. Para los críticos, la clasificación social puede determinar qué tan bien es tratado un usuario por todos aquellos otros con quienes se relaciona, o simplemente todo lo contrario; se argumenta sobre la posible formación de sistemas de castas en los medios de comunicación social, donde las personas con puntuaciones más altas reciben un trato preferencial por parte de las tiendas, posibles empleadores, etc. Si bien la puntuación es subjetiva y, por ahora, imperfecta dado que la mayoría de las empresas carecen de análisis de

sentimientos de las actualizaciones de los usuarios, por lo que una persona que genera una gran cantidad de charlas digitales puede recibir una puntuación alta a pesar de que lo que se dice sobre el usuario es negativo, o puede conseguir una puntuación alta si llegase a publicar un video que se replique en forma viral.

Como vimos antes, la Sra. Allison intentó jugar con los resultados de las búsquedas de sí misma buscando mejorar su reputación, pero se transformó en un trabajo tan arduo que llegó a considerar el dejar Internet. En lugar de eso, resolvió ponerse en contacto con gestores de reputación online para trabajar en su presencia en línea y una reputación difamada en la web. Los gestores de reputación online explotan los motores de búsqueda como Google y Bing mediante un conocimiento más profundo de la forma en que éstos trabajan, clasificando las páginas web basadas en la frecuencia con la que están vinculados desde otros sitios, e incluso creando páginas web tontas con contenido positivo para la reputación de sus clientes y aprobados por éstos. También llegan a contactar con webmasters o bloggers directamente, sobre todo en sitios más pequeños, y piden que se retiren puntos específicos de ciertos contenidos. Algunos sitios son más difíciles de modificar que otros: mientras que Wikipedia puede ser editada por cualquier persona, el borrado de una imagen de Google escapa a nuestro control.

Este servicio puede ser dado por una empresa con varios empleados u ofrecido por un solo programador experto y algún profesional externo. El precio de tener una buena imagen en línea

es muy variable, desde unos cientos de dólares al año, hasta miles de dólares para las celebridades, políticos y ejecutivos de alto nivel, debido al riesgo que conlleva una mala reputación y al mayor esfuerzo y fineza requeridos para el trabajo.

Al ser cada vez más la cantidad de información que compartimos en la red vivimos una época en la que la reputación de una persona se define por el comportamiento en Google, Facebook, eBay, y/o Twitter; y en donde es necesario pensar dos veces si realmente queremos subir esa foto o hacer ese comentario, porque la red no olvida y la información permanece por siempre, en servidores escondidos y protegidos bajo un entramado de hiperenlaces.

6. SEGURIDAD DE LOS JÓVENES EN INTERNET

Las estadísticas demuestran que la gran mayoría de los adolescentes hacen uso de Internet sin la correcta supervisión por parte de los adultos; quizás esto se pueda deber en muchos casos a que estos jóvenes tienen mayor conocimiento de la red que sus propios padres. Ante los riesgos que esto supone, distintas organizaciones internacionales tratan de concientizar de los peligros existentes en la red y en el uso indebido de ésta con campañas de comunicación dirigidas tanto a los propios adolescentes como a sus padres.

Así como vimos y hablamos de TinkB4UPost, existen otros anuncios sobre las consecuencias de subir fotos o publicar comentarios. Estos generalmente recogen historias breves protagonizadas por jóvenes que se enfrentan a peligros derivados del mal empleo de Internet, y ante los que casi siempre se han visto expuestos. Esta forma de llegar al público objetivo contando una historia en lo que se conoce como Storytelling es la más aceptada y la que mejores resultados ha demostrado. Algunos de estos anuncios ejemplifican en el plano físico lo que ocurre en Internet con el objetivo de que se comprendan con facilidad las consecuencias de subir fotos o de hacer comentarios en línea que pueden llegar a ser perjudiciales para el propio individuo o para otros. Campañas que muestran un sencillo error de presionar

enter y la foto es pública, o el creer que conocemos a la persona del otro lado de la pantalla, creer que se tiene el control de la situación; y muchas más que se pueden verificar de forma sencilla haciendo una búsqueda en Youtube sobre “Internet”, “riesgo”, “jóvenes”, “campaña”, “seguro” y combinaciones de estas palabras para que devolverán una cantidad importante de videos.

Según un reciente informe de Pew Internet & American Life Project, los datos son inequívocos, la mayoría de los jóvenes que utilizan la red son productores de contenidos. Dado que éste es uno de los usos fundamentales que hacen de Internet, enseñarles a hacerlo de forma segura debe formar parte de la educación en las aulas y en el hogar.

Existen varios organismos internacionales que están poniendo énfasis en la protección de datos personales, la educación y la seguridad en Internet. El mensaje principal que estas organizaciones transmiten es la crítica a la desinformación con la que niños y adolescentes acceden diariamente a las redes sociales y a los distintos contenidos que en ella se encuentran. Estas instituciones nacen con el objetivo de denunciar situaciones de desprotección sufridas por niños y adolescentes en todo el mundo. Algunas como Insafe son de carácter supranacional y pueden llegar a englobar a organizaciones nacionales sin ánimo de lucro y organismos públicos. Insafe es la principal institución en la Unión Europea y reúne centros de denuncia de 27 países europeos, de la comunidad y fuera de ella que a su vez en

algunos casos están formados por varias organizaciones dentro de cada país. Entre estos centros nacionales están la española Protégeles, la francesa Internet Sans Crainte y la británica Child Exploitation and Online Protection Centre (CEOP).

Otra de estas organizaciones es Pantallas Amigas, que tiene como misión tal cual lo dice en su web, la promoción del uso seguro y saludable de las nuevas tecnologías y el fomento de la ciudadanía digital responsable en la infancia y la adolescencia. Busca evitar los riesgos de un uso indebido de la tecnología, no sólo de la web sino también móviles u otros medios online, y de no ser posible esto, minimizar las consecuencias del mal uso de estas. Una de las iniciativas de esta organización es cuidatuimagenonline.com donde el eslogan igual que vimos en Insafe es "piensa antes de publicar". Basándose en un aprendizaje lúdico, utilizando juegos y multimedia intentan educar a los más jóvenes en los conceptos más importantes a tener en cuenta en su presencia en la red de redes.

También está embarcada en estos asuntos la Defensoría del Pueblo de la Ciudad de Buenos Aires, específicamente en el área de Protección de Datos Personales en la Infancia y la Adolescencia, donde alojan una campaña en que el slogan dice "Mostrate como sos pero… tus cosas son solo tuyas hasta que las subís a la red. Tu seguridad depende de vos" (muy clara la idea).

Todas estas asociaciones u organizaciones y sus campañas para informar y concientizar apuntan a los mismos conceptos, no enviar imágenes, ni dirección o teléfono, ni ningún otro dato

confidencial a desconocidos. Lo mejor es sólo compartir información con amigos, gente en quien confiemos. Las contraseñas que se utilicen deben ser siempre secretas y manejadas solamente por uno mismo, si consideramos que una contraseña puede verse comprometida, o existe alguna duda sobre si alguien pudo haber ingresado con ella, es conveniente cambiarla lo antes posible. Evitar encuentros personales con alguien que hayamos conocido en la red y si se decide ir es mejor hacerlo acompañado por un adulto. De ninguna manera debe divulgarse la información confidencial de los amigos y/o compañeros, ni publicar una foto o una grabación sin su permiso. Es importante recordar que tener permiso para sacar una foto no significa que puedas hacerla pública. Y finalmente el concepto central siempre es “no exponer los datos personales es la mejor manera de prevenir los riesgos de un mal uso de Internet”.

Una gran parte del presupuesto de estas organizaciones se destina a las campañas de comunicación para alcanzar los objetivos buscados, principalmente sobre la necesidad de contar con un Internet más seguro. En el caso de Insafe, casi la mitad del presupuesto se destina a este tipo de campañas, que incluyen desde anuncios en televisión o en Internet, programas informativos en centros escolares y el establecer redes internacionales públicas y privadas para fomentar la protección de los adolescentes y niños en el uso de la tecnología. A modo de ejemplo del mensaje trasmitido, algunos de los problemas más tratados son el ciberacoso, que es uno de los principales problemas sociales a los que se enfrentan los adolescentes, la

pérdida de privacidad, quizás el más difícil de comunicar y hacer comprender a los jóvenes, y la necesidad de una correcta supervisión en el hogar. Estas organizaciones han informado el éxito de una serie de anuncios que empleando la ironía para exponer la pérdida de control y la sobreexposición originada por el contenido personal en Internet, intentan mostrar contando una historia, trasladando las experiencias o vivencias del plano físico a lo que ocurre en la Red. Otro tipo de anuncios son aquellos que reflejan la brecha entre generaciones y muestran a padres e hijos enfrentando distintas situaciones difíciles por la falta de comunicación y conocimiento de Internet. Se busca a través de éstos movilizar a los padres y generar la idea de que es necesario compartir momentos frente a la pantalla con sus hijos.

Una de estas organizaciones en España y América Latina es Generaciones Interactivas, integrada por empresas, centros de enseñanza y gobierno. Su misión, según dice la web, es promover un uso de la tecnología que haga mejores a las personas. El foro busca fomentar la implicación activa de la familia, la escuela y la sociedad en la búsqueda de sus objetivos.

El documento publicado sobre Menores y Redes Sociales de Generaciones Interactivas, muestra que las estadísticas apremian para tomar medidas y comenzar a educar tanto a los jóvenes como a sus padres. Como dijimos anteriormente, la gente ha comenzado a vivir una parte mayor de sus vidas online, pero en los jóvenes los niveles de adopción son mayores aún. Más del 75% de los adolescentes dice tener un perfil creado en al

menos una red social, un 90% afirma tener en su casa un ordenador, el 60% tiene un teléfono móvil y más del 70% tiene conexión a Internet.

Dentro de los principales riesgos que existen en la red, la mayor cantidad de denuncias que recogen estas asociaciones son las relacionadas con la pornografía infantil, pero los riesgos son muchos más variados aunque muchas veces no llega a existir una denuncia concreta. El grooming consiste en que un adulto intenta contactar a un menor para tener contactos sexuales. Esto aunque no se quiera creer es cada día más habitual. Por otro lado tenemos el ciberbulling, que trata de utilizar la red para dañar y calumniar a otras personas y es otro de los hechos más repetidos entre los jóvenes. Son muchos quienes han sido víctimas de insultos por parte de otros internautas e incluso algunos dicen haber tenido miedo en alguna ocasión de acciones en el plano físico. Una situación también repetida en forma cada vez más común es la difusión de datos personales así como de imágenes comprometidas. Esto se repite entre los jóvenes, tanto compartidas por ellos mismos como por otros usuarios, otros jóvenes ejerciendo el ciberbulling, para exponer a la persona en la red, o no, simplemente porque tengo la foto y la publican (aunque como ya dijimos tener permiso para tomar una foto no significa poder hacerla pública). Toda esta realidad es la que reflejan las campañas de concientización que mencionamos, todos estos riesgos y acciones son las que se muestran y las que debemos tratar de que se entienda existen y para las que debemos estar preparados.

Los jóvenes se acercan a Internet mayoritariamente para usar los distintos servicios como forma alternativa o complementaria de ocio a las ya existentes, y sucede esto sin el debido conocimiento de las repercusiones o la resonancia que su actividad o sus acciones en la red pueden generarles. Internet es una herramienta muy útil pero hay que educarlos en su correcto uso. Existen distintos documentos tanto para padres como para jóvenes que ilustran y/o informan sobre un uso adecuado o simplemente dan una serie de recomendaciones, estos se pueden acceder en los sitios de las organizaciones o haciendo una simple búsqueda en la web por ejemplo de “Manual para Padres en Internet”. Lo principal es educar para que los jóvenes sepan ver una foto, y puedan pensar si es perjudicial o no y puedan decidir por si mismos si es mejor no subirla a la red.

Como se mencionó anteriormente uno de los factores que permite esta situación es la brecha digital existente entre padres e hijos. A diferencia de épocas antiguas, y no tan antiguas, en que el conocimiento se trasmitía de generación en generación, donde los mayores enseñaban a los jóvenes, los instruían y trasmitían su conocimiento basados en sus experiencias; a raíz de un cambio tecnológico que se ha dado con tanta rapidez estamos viviendo una situación que no se ha dado muchas veces en la historia humana, una época donde son los hijos quienes saben más sobre algo que sus propios padres, y son ellos quienes muchas veces deben trasmitir ese conocimiento. Sin lugar a dudas esto les impide a los padres abordar el tema de forma segura, utilizando la experiencia vivida como forma de manejar la situación y

dejando así navegar sin control a sus hijos. Eran los padres quienes enseñaban a sus hijos sobre los peligros en el uso de cualquier cosa que fuese necesario, desde caminar, andar en bici, jugar en la calle, etc. Hoy son los hijos quienes dominan la tecnología, jóvenes nativos digitales con una velocidad para asimilar el conocimiento mucho mayor a la de sus progenitores.

Por estos motivos, una de las recomendaciones que nos hacen desde estas asociaciones es la de conversar con nuestros hijos respecto a la navegación que se ha realizado por la red, de igual modo que nos debemos interesar por el resto de las actividades que estos realizan habitualmente en su vida cotidiana. También es posible instalar programas de protección de menores en nuestros computadores personales como ser Control Parental o Family Safety; pero a juicio personal esto no resuelve el problema, dado que no educa a los jóvenes, simplemente buscarían otro computador o dispositivo donde conectarse a la red.

Un punto importante que no debemos olvidar es el exigir que todas las empresas de la web 2.0, especialmente las redes sociales, se comprometan a respetar las leyes de Protección de Datos y de Protección de la Infancia y la Adolescencia. Los datos personales proporcionados a las redes sociales son habitualmente accesibles para todo el mundo, o presentan poca restricción, aunque ya varios de estos sitios tengan definido que estos datos sean de acceso privado o puedan configurarse por parte del usuario los niveles de privacidad deseados, lo que los deja

librados a la decisión de cada uno en su configuración de privacidad; y como ya dijimos anteriormente, estos datos pueden permanecer en la red para siempre.

7. PRIVACIDAD DE DATOS PERSONALES EN FACEBOOK

Volvamos sobre un caso puntual, no es algo contra Facebook que no se malentienda, es simplemente que ésta es la red social con mayor cantidad de usuarios registrados y que acceden con periodicidad, y por consiguiente la más utilizada. Según los rankings de Alexa, Facebook es el segundo sitio web con mayor tráfico a nivel mundial solamente superado por Google, adelantándose a sitios como Youtube, Yahoo o Wikipedia, y siendo en la mayoría de los países de América Latina el sitio número uno, el más visitado de todos.

Para ponernos un poco en contexto de esta red social estuve buscando datos, y encontré por ejemplo que más de la mitad de la población del Reino Unido tiene un perfil en Facebook, lo que es impresionante es que más de la mitad de estos, dicen usar la red social todos los días. En InsideNetwork encontramos reportes de los países con más actividad. Si bien Estados Unidos es el país con mayor cantidad de usuarios superando los 150 millones, Indonesia registra más de 40 millones, Turquía en el entorno de los 30 al igual que India, Méjico sobrepasa los 25 millones, Francia como Italia y Brasil tienen más de 20 millones de usuarios registrados. Todo esto a modo de ejemplo, además de que en cuanto terminé de escribir este párrafo las cifras ya eran caducas.

Muchos se refieren a Facebook como un país de casi 1000 millones de habitantes, por lo que no es de extrañar que las empresas se hayan volcado hacia allí, intentando atraer el interés de ese mercado masivo de individuos que utilizan la red social para ser conducidos a Internet y a sus amigos.

La manera en la que esta red funciona la hace viral, la forma de ver lo que otros están haciendo en ella es creando una cuenta personal, luego es necesario tener algo que mostrar a los demás de manera de no quedar fuera de onda. Lo siguiente después es intercambiar invitaciones de amistad con personas de tu pasado y de tu presente, y de muchos otros a los cuales no conoces. Si tus amigos tienen hijos, probablemente éstos también solicitarán ser tus amigos en Facebook, al parecer esto es genial para acumular miles de amigos, como una especie de ratings de la condición social, o de popularidad. Luego viene una avalancha inevitable de comentarios sobre tu muro, solicitudes para participar en juegos en línea, las miles de fotos de bebés que dan vueltas por tus contactos, recomendaciones de libros, las rutinas diarias de difusión en la plataforma, y un sin fin de cosas más.

Después de haber escrito y discutido varias veces sobre como las redes sociales borran la frontera entre la vida pública y la privada, y como cada uno de nosotros los usuarios somos quienes debemos poner este límite, sigo sintiendo que la gente no entiende y vuelvo nuevamente sobre lo mismo con una pregunta que encontré en Internet una vez: ¿cuánta seguridad tiene nuestro amigo más tonto?

Hemos estado discutiendo sobre la seguridad o privacidad en los medios de comunicación sociales y puntualmente sobre qué tan seguro puede ser Facebook como red social. Las personas tienen la idea o preconcepto de que Facebook puede ser seguro, ya que se puede restringir el acceso a nuestros contenidos, hacerlos visibles para quienes queramos y tener niveles de seguridad que filtren lo que otros pueden ver, ya sean amigos, amigos de amigos o cualquiera, incluso ahora la creación de grupos y la posibilidad de restringir a quiénes van dirigidas nuestras actualizaciones, tanto por grupo como individualmente por personas.

Sabemos que una cadena es tan fuerte como su eslabón más débil, y en términos de redes sociales, el eslabón más débil es el amigo con la peor o mejor dicho con la más débil configuración de privacidad y seguridad personal. Si bien podemos pensar que sabemos quiénes son nuestros amigos, no sabemos realmente qué tanto les preocupa o cuánto se involucran en su configuración de privacidad y seguridad en línea, qué cosas les conciernen a todos ellos, o que tanto saben de como mantener la privacidad en sus perfiles de usuario.

Dadas las políticas de acceso cada vez más intrusivas que están siendo adoptadas por los proveedores de tecnología de redes sociales, todos hemos aumentado potencialmente nuestra vulnerabilidad sin saberlo. A pesar de que Facebook ha proporcionado a sus usuarios nuevas herramientas de control sobre quién ve la información personal y cómo se utiliza, nuestra

red social sólo será tan segura como la seguridad de nuestro amigo más permisivo, y hasta de la forma en como este comente y/o recomparta nuestra información, y eso es una realidad peligrosa.

Esta situación es como tener un amigo chismoso, ese al que le decís algo y lo cuenta sin reservas, pero sólo que esta vez sale corriendo a gritárselo a todo el mundo; por ejemplo te ganas la lotería y se lo contás a este amigo, y este sale a la calle y lo grita, lo repite en todas partes, lo cuenta incluso a empresas con las que tanto él como vos se relacionan. Esta realidad también incluye a las aplicaciones que tenemos cargadas en nuestros perfiles, así como las de nuestros amigos también. Si bien se puede configurar la privacidad o la información que compartimos con ellas; muchos permisos son exigidos obligatoriamente y en ese caso algunos son importantes y comprometen nuestra información.

En el registro de acceso a la plataforma se muestra la información sobre nosotros y sobre nuestros amigos que ha sido solicitada por las diferentes aplicaciones que cargamos en nuestros perfiles de usuario. Podemos utilizar la página de Configuración de la aplicación para controlar cuáles de estas pueden acceder a tu información, a qué información acceden y lo que es muy importante que acciones pueden realizar en tu nombre. Las aplicaciones que utilizan tus amigos también pueden acceder a la información de tu perfil. Es importante conocer ese punto y saber cuáles de ellas solicitan acceder a nuestra información y a que

información acceden, de manera de saber lo qué están solicitando conocer de nosotros a través de nuestros contactos.

Esto es posible debido a que dentro de los permisos que damos a la aplicaciones está el de “Acceder a la información de mis amigos”, lo cual es obligatorio en algunas de ellas: cumpleaños, creencias religiosas e ideología política, familiares y situación sentimental, información de pareja, ciudad de origen, ciudad actual, gustos, música, televisión, películas, libros, citas, actividades, intereses, historial educativo, historial laboral, estado de conexión, sitios web, grupos, eventos, notas, fotos, videos, fotos y videos de amigos, estados de Facebook, etc. Si bien podemos configurar los permisos sobre qué información pueden ver las aplicaciones a través de tus amigos, hay que entender que la opción por defecto es bastante amplia, y aunque no queramos reconocerlo la mayoría de los usuarios la dejamos tal cual viene configurada originalmente desde la plataforma.

La privacidad es algo que todos debemos valorar, pero a menos que sepamos cómo hacer uso de su configuración en Facebook y en otras redes sociales en las que participemos, la información o los datos personales se pondrán a disposición de cualquier persona, aplicación o empresa que sepa cómo hacerlo o simplemente la solicite mientras esté en las opciones por defecto de la red.

Según un informe del PEW Research en general más allá de edad o sexo encontramos que para las configuraciones básicas de privacidad entre un 20 a 25% de los usuarios utilizan perfiles

totalmente públicos, entre otro 20 a 25% tienen configuraciones de privacidad parcialmente privadas y la mayoría, entre el 50 y 60% de los usuarios, han restringido el acceso a su información a los amigos, en lo que se considera una configuración de privacidad con un perfil privado, quedando clara la preocupación que tiene la gente en este sentido.

Facebook anunció una actualización de su plataforma en un post en su blog el 14 de enero de 2011. Una de las modificaciones fue permitir a las aplicaciones y otros sitios web externos acceder a esta información si el usuario les dio permiso, algo que ocurre al momento de agregar una aplicación a tu perfil. La controversia sobre esta nueva característica es otra perla en una larga y dudosa historia sobre políticas de privacidad de la empresa, que por otra parte recientemente lanzó un formato de prueba de su política de privacidad que aparentemente es más sencilla de comprender para los consumidores sin formación jurídica, algo que probablemente lo que la gran mayoría de los usuarios estábamos esperando.

Como ya se mencionó anteriormente, algunos empleadores han visitado la página de Facebook de potenciales empleados para ver su información pública, incluso se ha conocido algún caso en el cual el empleador exigió el acceso al perfil de un usuario antes de su contratación, como ocurrió con un hombre en los Estados Unidos específicamente en el estado de Maryland, Estados Unidos, que se encontraba haciendo una recertificación en su trabajo en el Departamento de Correccionales del Estado (servicio

penitenciario) y durante la entrevista le exigieron revelar sus credenciales en Facebook, el nombre de usuario y la clave, con la increíble intromisión a la privacidad que esto conlleva. Es como tener que entregar toda la correspondencia y las fotos privadas que tengas en tu casa, como describe la carta enviada por la Asociación de Libertades Civiles del Estado de Maryland ACLU, esta actitud es una invasión a su privacidad y a su vida fuera del trabajo. Otros empleadores simplemente han intentado mediante un perfil falso o un perfil válido generar un vínculo de amistad para acceder a la información, argumentando en todos los casos que era para chequear conocimientos y aptitudes, pero presumiblemente para ver lo que este candidato actualizó de su vida privada, dando acceso a las publicaciones en el muro, los juegos, la música, grupos a los que se pertenece y a toda la información que cada uno expone de sí mismo a su círculo de amistades.

No debemos olvidar que la mayoría de las redes sociales, o quizás todas las que son usadas en forma masiva son gratuitas, sin costo para los usuarios y tienen que ganar dinero de alguna manera. Al crear un usuario aceptas condiciones de servicio, y estas pueden ser simplemente el seguimiento de los clicks en sus propias herramientas de medición interna, pero también puedan incluir la recopilación de datos para venderlos a anunciantes, e incluso podrían también vender la información de contactos a un tercero.

Por más que lo repita mil veces no me voy a cansar de recordarles que es necesario leer las condiciones de uso y ver a qué nos exponemos, dado que el objetivo principal de las redes sociales es ayudarnos a mantenernos conectados y comunicados con otras personas, la configuración de privacidad en la mayoría de las redes sociales por defecto se configuran como una opción amplia y abierta. Para que se pueda mantener cierto grado de intimidad en éstas se necesita mucho esfuerzo y a menudo esta acción es contraria a los objetivos del servicio, que se brindan sin costo ya que están vendiendo el acceso a nuestra información.

Con la necesidad del desplazamiento a través de kilómetros de jerga legal, la mayoría de los usuario optan por la ignorancia y hacen click en "Estoy de acuerdo" sin leer una sola palabra de lo que están aceptando, y realmente todos lo hemos hecho alguna que otra vez. La mayoría de las veces no hay consecuencias negativas, pero de vez en cuando, sin saber que estamos aceptando y a lo que nos estamos comprometiendo podemos llegar a tener problemas. Como ejemplo está este texto, parte del acuerdo de términos y condiciones que los usuarios de Facebook aceptamos al crear nuestros perfiles en la red social y de los compromisos que asumimos al pertenecer a ella:

“Sobre el Compartir el contenido y la información, los documentos de Facebook dicen que eres el propietario de todo el contenido y la información que publicas en Facebook, y puedes controlar cómo se comparte, además para el contenido protegido por derechos de propiedad intelectual, como fotografías y videos (en

adelante, "contenido de PI"), nos concedes específicamente el siguiente permiso, de acuerdo con la configuración de privacidad y aplicación: nos concedes una licencia no exclusiva, transferible, con posibilidad de ser sub-otorgada, sin royalties, aplicable globalmente, para utilizar cualquier contenido de PI que publiques en Facebook o en conexión con Facebook (en adelante, "licencia de PI"). Esta licencia de PI finaliza cuando eliminas tu contenido de PI o tu cuenta (a menos que el contenido se haya compartido con terceros y éstos no lo hayan eliminado). Cuando eliminas contenido de PI, éste es borrado de forma similar a cuando vacías la papelera o papelera de reciclaje de tu equipo informático. No obstante, entiendes que es posible que el contenido eliminado permanezca en copias de seguridad durante un plazo de tiempo razonable (si bien no estará disponible para terceros). Cuando usas una aplicación, tu contenido e información se comparte con ella. Exigimos que las aplicaciones respeten tu privacidad y tu acuerdo con esa aplicación controlará el modo en que la aplicación puede usar, almacenar y transferir dicho contenido e información. Cuando publicas contenido o información con la configuración "Todos", significa que permites que todos, incluidas las personas que son ajenas a Facebook, accedan y usen dicha información y la asocien a ti (es decir, tu nombre y foto del perfil). Siempre valoramos tus comentarios o sugerencias acerca de Facebook, pero debes entender que podríamos utilizarlos sin obligación de compensarte por ello (del mismo modo que tú no tienes obligación de ofrecerlos)".

La verdad es que utilizamos redes sociales todo el tiempo, generalmente sin considerar verdaderamente los riesgos que esto trae consigo, sin siquiera pensar cuánta información personal es almacenada, así como el hecho de que por más que tengamos la configuración de privacidad activa, esto no significa que estemos completamente protegidos. El acuerdo de partes que aceptamos al registrarnos por el cual la red social nos permite compartir información con quienes nosotros queramos y ellos pueden usar esa información para decidir que publicidad mostrar, y que involucra como en todas las relaciones la confianza entre las partes, es algo que muchas personas desconocen por desinterés a la hora de registrar sus cuentas: ¿realmente queremos que toda esa información este allí pública o sem-pública? Personalmente estoy convencido de que no todo debe ser compartido.

Facebook ha logrado persuadir a millones de personas que participen subiendo a la red información acerca de ellos mismos bajo un disfraz o manto de privacidad que en realidad está lleno de huecos más parecido a un colador que a un muro y por el cual la información se filtra por muchas partes. En setiembre de 2011 la empresa introdujo varios cambios a estas políticas, como generalmente sucede estos cambios vienen acompañados de quejas y nuevas preocupaciones acerca de la privacidad. Como ya hemos dicho, la red social almacena, registra y recuerda todo lo que hacemos en ella, y con los nuevos cambios por ejemplo en la Timeline se lo cuenta a todos, mantiene el registro de todo lo que hemos publicado nosotros mismos o compartido a través de otros amigos.

Facebook esta allí observando cada cosa que hacemos. La herramienta de reconocimiento de rostros o facial es utilizada para identificarnos en las fotos y ofrecerles a nuestros amigos que nos etiqueten en ellas, no es que sea la única red social que la tenga, pero como ya dijimos es la más grande. Por otro lado está adivinando los intereses y gustos o preferencias basándose en los de tus amigos, incluso si no has proporcionado ningún dato al respecto.

Se ha ampliado la información personal de los usuarios que comparte la red con la comunidad de desarrolladores y se ha incluido el número de celular y otro tipo de información de contacto en ella. Esto es más peligroso ya que en esta plataforma de desarrollo también se puede encontrar software malicioso, aunque la empresa intente evitar este tipo de situaciones, las consecuencias pueden ser muy negativas para los usuarios.

Más allá de Facebook Places, la red social permite que al escribir una actualización de estado, subir una imagen o cualquier cosa que publiquemos se pueda compartir tu ubicación geográfica con el mundo o con quienes puedan llegar a verla, con su peculiar perjuicio para la privacidad de ubicación, dado que esto también va incluido en la timeline. El seguimiento de tus hábitos de navegación, gustos o preferencias mediante el botón “Me gusta” ubicado en otros sitios web es considerado ilegal y conlleva una multa en países como Alemania.

Hace un tiempo Facebook debió reconocer públicamente que algunas aplicaciones en su sitio, incluido el popular juego

Farmville, el más popular de la red social con más de 60 millones de usuarios, habían compartido incorrectamente la información de identificación de los usuarios y en algunos casos la de sus amigos, con anunciantes y con compañías de seguimiento de la web. Debieron sacar un comunicado de prensa informando que estaban acordando con los desarrolladores de aplicaciones sobre cómo se debe manejar la información personal para evitar que esto volviera a suceder.

Una serie de artículos del periódico The Wall Street Journal ha revelado como Facebook maneja la información personal de sus usuarios y los usuarios hemos descubierto que aparentemente la red social ha estado tomando con ligereza este tema. Se ha encontrado que las diez aplicaciones más populares de Facebook han estado compartiendo nuestra información personal con empresas de mercadeo y publicidad, algo que viola las políticas de privacidad de esa red social, e incluso han compartido los datos de los amigos de sus usuarios, aunque estas terceras personas ni siquiera estén utilizando esas aplicaciones. El periódico afirmó que la fuga de datos habría afectado a decenas de millones de usuarios, incluyendo a aquellos que tienen activadas las más fuertes medidas de seguridad para resguardar su información privada, varias organizaciones incluyendo a la EEF (Electronic Frontier Foundation) calificaron el hecho como de extremadamente serio.

Como ya veremos más adelante la información aislada no es tan útil, pero si obtenemos varios trozos de información se pueden

hacer cosas importantes, en este caso los anunciantes y las empresas de rastreo pueden asociar estos datos de los usuarios de Facebook con la información que ellos han almacenado y conseguir de esa forma un valor mayor de éstos y una ventaja de negocios. Esta información fugada es algo así como darles una llave mágica para poder hacer un seguimiento de los usuarios con mayor profundidad en la cantidad y calidad de la información recogida y a recoger en el futuro.

Alemania ha llegado a considerar que la utilización de Facebook involucra un riesgo para los usuarios. Según manifestó Andreas Vosskuhle, Presidente del Tribunal Constitucional de Alemania, "con las condiciones actuales usar Facebook podría significar una actividad de riesgo para los usuarios", al considerar que estos pierden el control de sus datos una vez que son publicados. Incluso los usuarios desconocen si los datos se han eliminado realmente después de haberlos dado de baja. La red social ya ha tenido varias polémicas en este país, donde no se ven con buenos ojos algunas de las prácticas que la compañía realiza en estos asuntos.

Los ciudadanos desconocen si los datos son eliminados después de haberlos retirado de la red social, lo que es una prueba de la pérdida de control de su información. La justicia alemana ha considerado que algunas prácticas de Facebook están en contra de leyes del país, que éstas tendrían que ser reformuladas de forma de presentar una posición clara en materia legislativa ante las redes sociales e Internet en general. También se ha advertido

del peligro que entraña para los usuarios alemanes el que Facebook decida llevar sus servidores fuera del país, entendiendo que establecerse fuera del alcance de la jurisprudencia alemana podría generar un peligroso desequilibrio entre el poder de Facebook y las posibilidades de emprender acciones legales por parte de sus ciudadanos de ese país.

Además de Alemania individualmente, la Comisión Europea en su conjunto pretende exigir (o ya lo está haciendo) a los sitios de Internet que almacenan información de sus usuarios, que eliminen los datos personales de éstos al darse de baja de sus servicios, en vez de conservar toda la información. Aunque estas empresas estén fuera de la Unión Europea, la medida afectaría a todos los perfiles de ciudadanos europeos existentes en sus plataformas. Esto no sólo incumbe a Facebook sino a otros gigantes de la red como Google, quienes tendrán que modificar sus sistemas para cumplir con la norma. Al día de hoy, cuando un usuario abandona la red social, su perfil permanece intacto, de forma que sólo basta con reintroducir el viejo nombre de usuario y la contraseña para reingresar en él, y recuperar toda la información que estaba disponible al momento de darse de baja. Las fotografías y la información siguieron en la red, incluso si no se había restringido la privacidad del perfil, es posible encontrar todos los datos e imágenes que contenía, simplemente haciendo una búsqueda en la web por el nombre del usuario.

Max Schrems, estudiante de derecho Austríaco, es una de las pocas personas que han logrado que Facebook le proporcione una

compilación completa de sus datos personales. Esta compilación resultó ser un archivo de 1.222 páginas en el que figuraban todas sus actividades en la red social, incluyendo aquellas cosas que creía haber borrado. La información le fue dada desglosada en 57 categorías distintas, incluidos sus gustos, los accesos a la red con la lista de direcciones IP utilizadas, entre otras tantas cosas. Lo que sucede es que los datos no son realmente eliminados del sistema, sino que más bien quedan escondidos en una especie de limbo, esperando a ser recuperados si su propietario solicita crear la cuenta de usuario nuevamente, y ¡"voila"!, todo está allí nuevamente disponible. Esta opción parece ser útil para quién luego de borrar su usuario cambia de opinión y pretende recuperar la cuenta, también recuperará sus amigos, sus fotos y todo lo demás, no es necesario empezar de cero.

Habiendo estudiado el tema durante su carrera en la universidad, Schrems entendió que la red social violaba 22 disposiciones vigentes en la Unión Europea, y procedió a denunciar a Facebook en agosto de 2011 por conservar datos personales sobre su vida privada que él mismo había suprimido, esta denuncia fue presentada ante la Autoridad de Protección de la Vida Privada de Irlanda que es el país donde la red social tiene su sede europea. La empresa podría enfrentar una multa de hasta 100 mil euros, si bien el tribunal en cuestión sólo puede comprobar la existencia de violaciones a las disposiciones vigentes y solicitar a la empresa que realice las modificaciones y/o correcciones necesarias, y si ésta no las hiciese recién en ese momento podrá llegar a aplicarle una multa.

Si la información es poder, la información sobre las personas es tener poder sobre éstas. Es aterrador que todos estos datos estén almacenados en Facebook por siempre. La propia red social ha informado que dispone en su sitio de una herramienta de modo que cualquier usuario pueda descargar su archivo personal, aunque algunos individuos preocupados por este asunto argumentan que la información que allí se descarga es solamente una fracción del total de los datos que la compañía almacena sobre cada uno de los perfiles.

Realmente podemos decir que las redes sociales tienen el poder sobre el contenido de los usuarios, por ejemplo, si la imagen de su perro se volvió un éxito entre sus amigos en Facebook, esta podría ser utilizada en un anuncio publicitario sin necesidad siquiera de que recibas una notificación, como está establecido dentro de los derechos compartidos sobre el contenido con derechos de propiedad intelectual. La red social también puede compartir estos derechos de uso con terceros, según lo definido dentro las políticas de privacidad y términos de uso de la plataforma.

No olvidemos un dato significativo: la posibilidad de realizar modificaciones en estos documentos o cualquier punto dentro de ellos sin necesidad de notificar a cada uno de los usuarios o simplemente realizando un aviso general al cual deberemos estar atentos y leer con atención. Este hecho ya ha acontecido en Facebook anteriormente e incluso en alguna ocasión han debido rever los cambios a razón de la oposición demostrada por una

gran cantidad de integrantes de la red social. Pero dejemos claro que esta regla no es aplicable solamente a Facebook, esto sucede en otras redes sociales, más bien en todas.

Nik Cubrilovic, un joven emprendedor y hacker australiano publicó en su blog un post sobre al hecho de que el cerrar sesión en Facebook no es suficiente, referida a una característica de las cookies permanentes que utiliza la red social, las que le permitirían conocer y llevar un registro de cada página que un usuario visita en su navegación web, incluso aunque hayas cerrado sesión en la red social. Casi de inmediato un ingeniero que trabaja en los sistemas de login de Facebook, Gregg Stefancik, respondió con un comentario en el post original del blog en cuestión, que comienza pidiendo disculpas por no haber sido explicito y comunicar correctamente las prácticas con respecto a las cookies, pero agrega una afirmación contundente que apunta a cambiar el eje de la discusión, diciendo que a diferencia de otros gigantes de Internet, ellos no están interesados en hacer un rastreo de las personas, que no poseen una red de publicidad con la que obtener ganancias de esta información y que no comparten los datos que recopilan con terceros para dirigir publicidad a los usuarios. Afirmación que por más que proceda de la empresa genera muchas dudas como es de esperarse, si no, ¿para qué hacen uso concretamente de cookies permanentes que permiten hipotéticamente llevar a cabo un seguimiento del usuario incluso cuando no está usando la red social? Posteriormente el autor escribe una actualización en la entrada sobre el tema tras clarificar algunos puntos con

Facebook, que además informa haber decido cambiar algunos aspectos de su proceso de logout para evitar un potencial mal uso de estas características referidas a las cookies.

Facebook presentó poco después de la salida de Plus, la red social de Google, o la capa social a las aplicaciones de Google, una serie de cambios en su plataforma. Las principales modificaciones que se implementaron fueron acuerdos con terceros para compartir contenido multimedia desde los perfiles de cada usuario con otras redes sociales de servicios como Spotify (música), Netflix (películas) y Hulu (programas de televisión). Se anunció un nuevo muro rediseñado para hacerlo mucho más atractivo gracias a las imágenes gigantescas que se podrán ver en él. Y por último, la timeline de actualizaciones o cronología que recuerda a los servicios que presta Twitter, informándonos en tiempo real de todo lo que están haciendo nuestros contactos en la red social y a éstos de todo lo que nosotros hacemos.

El objetivo perseguido con estos cambios es el obtener una mejora sustancial en la experiencia de los usuarios; sin embargo a poco de ponerse en producción, los usuarios de la red han manifestado su disconformidad con algunas características de estos cambios. Las principales críticas expresadas fueron la pérdida de privacidad, más allá del esfuerzo en crear una serie de herramientas que permitieran manejar de forma sencilla quién podía ver y quién no cada una de nuestras publicaciones, la llegada del 'feed' de últimas noticias ha atentado contra la privacidad. Ahora, todos pueden ver lo que hacemos en

Facebook, desde la canción que estamos escuchando en Spotify hasta las veces que pulsamos 'me gusta' en una foto, así como ver todo el contenido de las publicaciones con las que interactúan nuestros amigos.

Un ejemplo más simple para mostrar la intrusión en la información personal o el hueco generado en la privacidad por este cambio puede ser el acceso a una foto: si a un amigo nuestro le gusta una foto subida por una tercera persona a la que no conocemos y que no integra nuestra lista de amigos, podremos llegar a ver esa imagen haciendo click en ella cuando la red nos avise que a nuestro amigo le gusta esa foto, aunque ésta se haya configurado al momento de compartirla para que sólo la puedan ver los amigos personales de quien la agrega; reviviendo el hecho de que todo lo que subamos a Facebook puede llegar a ser público, o mejor dicho, tener un alcance muy diferente al que le quisimos dar.

Para modificar esta opción es necesario modificar las opciones de suscripción con cada usuario. Al estar suscrito puedes recibir noticias de la gente que te interesa, incluso si no son tus amigos, con quienes siempre has estado suscrito. Es una forma de recibir las actualizaciones públicas de personas que no son tus amigos haciendo uso de la opción de suscribirse en el perfil del usuario. Sólo si estos permiten suscripciones éstas aparecen en tus noticias. Para el caso de tus amigos, la opción por defecto es estar suscrito a "La mayoría de las actualizaciones". Para modificar esto, hay que pasar el ratón por encima del botón

"Suscrito(a)" en el perfil de un amigo y configurar las opciones deseadas. Por ejemplo, podemos desmarcar "Comentarios y Me gusta", o “Acontecimientos importantes”, “Actualizaciones de estado”, “Fotos”, “Juegos”, etc. El problema con esto es que la configuración de lo que puedo visualizar de mis contactos, o a través de ellos, lo defino yo y no el usuario realmente interesado en proteger su privacidad. Éstos son capaces de ver los comentarios y las fotos o actualizaciones de personas que están en un segundo nivel de amistad a través de las acciones de sus amigos, como el ejemplo que mencionamos, donde un amigo nuestro comenta sobre la foto de una tercera persona que no está entre nuestros amigos y al desplegarse en nuestra lista de noticias podremos acceder a la foto de ese tercero sin tener relación directa.

Como en toda herramienta informática existen fallos en la seguridad, que combinados con este deterioro de la privacidad pueden comprometer información sensible; como le sucediera a su fundador y CEO Mark Zuckerberg con la filtración a raíz de un fallo de seguridad en los servidores de varias fotografías privadas. Estas fotografías, de él con su novia y con amigos, estaban almacenadas en su perfil personal dentro de la red, y fueron hechas públicas. Todas estas fotos personales están disponibles en Internet en distintos blogs.

Las listas inteligentes son otra de las nuevas funciones que discuten los defensores de la privacidad. Éstas permiten organizar a nuestros amigos en función de diferentes criterios como el lugar

de estudio o parentesco. Si bien resulta bastante útil a la hora de realizar actualizaciones de estado y hacerlas visibles para estas listas o simplemente para mantener una organización de nuestros amigos, también significa dar a Facebook más información sobre nuestra red de amigos y conocidos, decirle quienes integran diferentes subgrupos, en función de qué criterios, y por consiguiente, representa una mayor vulnerabilidad de nuestra vida privada, principalmente ante la posibilidad de una eventual fuga de información de la red social.

Dentro de este ecosistema existe lo que se conoce como Socialbots. Estos son utilizados muchas veces para robar los datos de distintos usuarios en Facebook. Simulando ser verdaderas cuentas en la red social: usuarios reales y personas reales, son capaces de recolectar grandes cantidades de información personal. Si bien los responsables de la empresa han manifestado que la información o los datos que distintos informes dan sobre la existencia en capacidad y cantidad de estos bots son exageradas, esta técnica es utilizada por cyber delincuentes, y esta realidad es innegable dado que estos bots son una evolución de los ya utilizados a gran escala para el envío de spam.

Un bot tradicional, a menudo roba datos de los computadores de sus víctimas o utilizan sus máquinas para enviar spam o llevar a cabo otro tipo de ataques a terceros. Un socialbot podría tomar el control de un perfil en la red social y desde allí lleva a cabo actividades básicas como enviar mensajes y solicitudes de amistad.

En una reciente investigación llevada adelante por estudiantes de Doctorado de la Universidad de British Columbia en Vancouver y su profesor, se crearon socialbots para gestionar 120 perfiles falsos en la red social y un botmaster para la gestión de los otros robots. El tiempo de la investigación fue de ocho semanas, y en total estos sistemas trataron de hacer amistad con 8.570 usuarios distintos, enviando no más de 25 solicitudes diarias por perfil para evitar ser detectados por los sistemas antifraude de la red social. De los usuarios contactados, 3055 aceptaron el pedido de amistad, siendo más propensos a aceptar la falsa solicitud aquellos usuarios con mayor cantidad de amigos en su red personal.

En el documento presentado por los investigadores se describe como sus socialbots se infiltraron en la red con el objetivo de recopilar datos privados de los usuarios, tales como direcciones de correo electrónico, números de teléfono y otros datos personales que tienen valor monetario. Los investigadores afirmaron haber obtenido de la red de amigos y de la red extendida unas 46.500 direcciones de correo electrónico y 14.500 direcciones físicas.

Nuevamente los responsables de Facebook dijeron que el experimento no era realista, basados en que las direcciones IP utilizadas para la investigación procedían de una fuente de confianza como ser la universidad, mientras que de haber sido distinto, de haber realizado la investigación desde direcciones IP de clientes estándar, se hubieran disparado las alarmas de los

sistemas de seguridad y fraude, argumento que no parece ser muy descabellado. También se informó que habían sido desactivadas más cuentas falsas por parte de los sistemas que las informadas por los investigadores. El portavoz de la red social recomendó lo que el sentido común nos dice, una de esas cosas que personalmente siempre he recomendado y que se ha repetido varias veces, que los usuarios hagan lo que deben hacer, conectarse sólo con personas a las que realmente conozcan.

Los investigadores concluyen que la infiltración en redes sociales a gran escala es una de las muchas amenazas cibernéticas para el futuro, y la necesidad de contar con sistemas de defensa contra esas amenazas es una necesidad para poder considerar la web social más segura para todos los que las usamos. Lo que sí es evidente es que hay una lección para los usuarios de Facebook: deben aprender sobre la necesidad de tener especial cuidado y prestar atención en las relaciones de amistad en la red, además de cuál y qué tipo de información se decide compartir en línea.

Del mismo modo también podemos llegar a recibir una solicitud de un verdadero amigo por ejemplo para ver un video, el cual lamentablemente ha sido enviado por algún software malicioso que infectó el perfil de ese amigo y de sus amigos. Hay reportes de varias aplicaciones del tipo de “¿Quiere saber quién ha visitado su perfil?” Éstas no son otra cosa que software malicioso, este tipo de aplicaciones se propagan mediante la creación de eventos donde presentan a los usuarios la opción de poder saber o mejor dicho de poder informarnos quién entra en nuestra cuenta de

Facebook, o quienes han mirado las fotos. Al acceder, la página pide los datos de usuario y contraseña, en caso de aceptar la aplicación y seguir los pasos indicados el programa pasa a publicarse en nuestro muro, y reenvía la invitación a toda la lista de amigos sin la autorización del usuario, haciéndose con el control del perfil, teniendo acceso a información personal suya y de sus contactos. Estas aplicaciones se pueden eliminar como cualquier otra, en la sección de aplicaciones y sitios webs dentro de la configuración de privacidad de cada usuario.

Julian Assange, periodista y activista australiano conocido por ser fundador y editor en jefe de WikiLeaks, en entrevista para Russia Today ha dicho que las redes sociales son la máquina de espionaje más atroz jamás inventada. Para Assange, Facebook es utilizada por los servicios de inteligencia de Estados Unidos para tener a los ciudadanos controlados.

Pensar en Facebook como la base de datos de individuos más completa del mundo, con sus relaciones, sus nombres, sus direcciones, sus localizaciones, y hasta las comunicaciones entre ellos, y su red de amigos y en Internet como la máquina de vigilancia más importante que jamás hemos visto, en referencia a la cantidad de información que las personas dan de sí mismos en línea, resulta abrumador.

La respuesta de Facebook no se hizo esperar, y en una entrevista para Forbes un vocero de la empresa declaró que si bien es cierto que reciben muchas peticiones que solicitan información de sus usuarios, Facebook no procesa estos datos automáticamente.

Afirma que la empresa no responde a la presión, responde a los procesos legales, que son obligatorios. Las normas jurídicas para obligar a una empresa a entregar estos datos están determinadas por las leyes y éstas son respetadas.

Assange también afirma que realmente ésta es nuestra gran batalla: la tecnología da y la tecnología quita.

Debemos tener mucho cuidado con las configuraciones de privacidad y seguridad de nuestros perfiles, pero también hay que tener cuidado con lo que se dice y cómo se dice, así como con lo que se muestra en la red, allí todo es público. Es fundamental entender que si no queremos que mucha gente se entere de algo, lo mejor es no publicarlo, y entender que lo que subamos a la red puede volverse de alcance público aunque nosotros no lo hayamos querido así.

8. SOBREEXPOSICIÓN DE INFORMACIÓN

Hoy en día seguimos encontrando gente que considera a aquellas personas que están mucho tiempo conectados a Internet, en varias redes sociales, que utilizan la tecnología para comunicarse y relacionarse y que llevan una vida conectados a la red, como parias sin voluntad, desprolijos mal vestidos que se aíslan del mundo detrás de un computador. Yo sé que existen este tipo de personalidades, hoy al igual que en otras épocas de la humanidad con comportamientos similares. Pero la red es un complemento de nuestro ser social, es una extensión del sentido de pertenencia y nos brinda una herramienta increíble a la hora de seguir relacionados con aquellas personas con las que ya sea por el paso del tiempo o por la geografía que nos separa, nos hemos ido distanciando física y emocionalmente.

Personalmente me ocurre que a pesar de vivir de esto, de ser Internet mi trabajo y mí medio de sustento, cada vez que encuentro a alguna persona o me encuentran a mí, y retomo contacto con algún amigo del que hace tiempo no tengo noticias, me emociono de tal forma que me sorprende una y otra vez. El cómo Internet y las redes sociales mucho más, hacen que los sentimientos sigan presentes se vuelvan a vivir, y las personas no pierdan la oportunidad de relacionarse por la distancia o el tiempo es realmente genial. No soy el único que piensa así, la sensación

es similar en la mayoría de las personas: ¿cuántos han vuelto a reuniones de camaradería en el mundo físico con sus compañeros de escuela, a los que no veían desde esa época, y a los que encontraron a través de Facebook por ejemplo? En esta zona del mundo ese tipo de reuniones no era usual, pero los grupos se han vuelto a encontrar en Internet, y este tipo de experiencias se ha visto repetida una y otra vez y trasladada al mundo físico.

¿Esto usuarios frecuentes de las redes son parias que se aíslan detrás de un computador dentro de un mundo ficticio o son seres humanos a los cuales las redes sociales han potenciado su capacidad de interrelacionarse y de compartir información unos con otros? Hemos evolucionado para manejar una cantidad enorme de contactos y relacionarnos con personas que antes estaban física, temporal o geográficamente inaccesibles, y esta es una realidad que no va a disminuir, nos deberemos adaptar, hacernos un espacio y manejar nuestros contactos y la información para estar cada vez más conectados los unos con los otros y todos con la red.

Ya hemos discutido varios temas que nos han conducido justamente a este punto, compartir demasiada información. Intentemos dar una definición sobre de qué se trata este concepto para que quede más claro de lo que hablamos: la sobreexposición de información o como se conoce en la web por su nombre en inglés “oversharing information”, es considerado como el acto de compartir demasiada información personal en la

web, información que bajo ciertas circunstancias o usos nos puede llegar a resultar incómoda o sencillamente inaceptable.

La red toca casi todos los aspectos de nuestras vidas, desde la forma en que la aplicamos en el trabajo, dónde y como nos mantenemos informados, hasta la forma en que nos relacionamos con familiares y amigos. El cambio ha sido tan brusco, que algunas actividades que hasta hace poco eran de uso cotidiano han sido cambiadas por unos pocos sitios web, como por ejemplo la búsqueda de información en una enciclopedia o en la guía telefónica. Vivimos una época donde todos los seres humanos, incluso aquellos que no tienen contacto directo con la red están sujetos a un nivel de exposición pública impensable hace unos pocos años. La privacidad ha disminuido a niveles increíbles, la relación entre los distintos mundos en la vida de las personas es cada vez mayor, el hecho de cómo tu vida personal afecta tu vida laboral y viceversa ha variado sustancialmente en estos tiempos, asemejándose a la época en la que los seres humanos vivían en pequeñas aldeas donde todos conocían todo de cada uno de los individuos que pertenecían a su comunidad: si estaban enfermos, si comían, si trabajaban, absolutamente todo. El tamaño de las ciudades, la separación de los grupos de un individuo, laboral, familiar, amistad, etc. hicieron que se construyeran muros y sintiéramos cierto grado de privacidad, muros que Internet se ha encargado de derribar.

Entonces, ¿por qué un individuo puede asumir que las mismas leyes o normas sociales que protegen su privacidad en el mundo

físico se aplican al mundo digital? La realidad es que las normas o reglas relativas a la privacidad en línea están aún en desarrollo, por lo que como se mencionó en otros capítulos, aprender a navegar por Internet con seguridad es esencial para mantener nuestra privacidad lo más cuidada posible o dentro de parámetros que cada uno de nosotros debe fijarse para sí mismo.

Hagamos un repaso a algunas cosas y veamos qué acciones de las que hacemos en Internet revelan información, o que información estamos compartiendo en las distintas actividades que hacemos al navegar la web. Simplemente al estar en línea se proporciona información a cada paso del camino, generalmente se le pueden considerar datos sueltos y llegar a obtener algo significativo de todo esto puede ser como resolver un rompecabezas. La información que proporcionamos a una persona, empresa o sitio mientras navegamos puede no tener sentido alguno, a menos que se combine con la información que proporcionemos a otra persona, empresa o sitio web, o que éstas tengan un volumen y complejidad de información tan importante que la haga significativa, como puede ser el caso de empresas como Google o Facebook, y que puedan con estos datos hacer un verdadera ingeniería social para obtener información importante y útil acerca de sus usuarios.

Pensemos en un servicio masivo como el correo electrónico. Si bien ya han habido varias resoluciones de la justicia al respecto, el asunto tratado en estos casos ha sido la expectativa de privacidad que se concede al correo electrónico alojado en un

servidor remoto por parte de los usuarios. Para dar un ejemplo, en un juicio en 2010 el Sexto Tribunal de Circuito de Apelaciones de los Estados Unidos dictaminó que si bien un proveedor de servicios tiene acceso al correo electrónico privado, el gobierno debe obtener una orden de registro antes de acceder a esa información. Dadas las similitudes fundamentales entre las formas de correo electrónico y de comunicación tradicionales como el correo postal y las llamadas telefónicas, sería desafiar el sentido común dar a los mensajes de correo electrónico menor protección que al correo postal.

Si hablamos de una actividad básica como ser el navegar en Internet, aunque se piense que esto es algo anónimo, en realidad no lo es. Al navegar por la web se transmite información personal a cada sitio que se visita, proporcionamos datos básicos como ser la dirección IP, información del equipo que utilizamos y algunos datos más a cada uno de los operadores de sitios que visitamos. Si bien es posible configurar el navegador para restringir el uso de cookies y mejorar la privacidad, esto también nos quita algunas funcionalidades.

Muchos o casi todos los servidores que visitamos almacenan datos en nuestro computador relacionados con la navegación que hacemos en estos sitios, aplicaciones, etc. Estos datos se guardan en archivos llamados cookies, que son un fragmento de información que se almacena en nuestro computador desde una página web, esta información puede ser luego recuperada por el servidor en posteriores visitas. Estas pueden incluir información

como identificación o registro de entrada, preferencias del usuario, información en línea, etc. El navegador guarda la información y la envía de vuelta al servidor web cada vez que el usuario vuelve a la página del sitio dueña de la cookie. El servidor Web puede utilizar esta información para hacer un seguimiento de la actividad que tenemos en el sitio, y/o mantener ciertos valores de sesión que mejoren la experiencia del usuario, personalicen una página o hasta mantener datos en un carrito de compras. Estas cookies se llaman cookies de origen y son las más comunes.

Existen otras cookies denominadas de terceros, que envían datos acerca de nosotros para el intercambio de publicidad y comparten estos datos con otros sitios interesados en ellos. El navegador de Internet que utilicemos y algún otro software ya sea gratuito o pago permiten detectar y eliminar las cookies, incluyendo las cookies de terceros.

También como destino de nuestra información o como uno de los puntos neurálgicos donde dejamos datos personales, tenemos a los motores de búsqueda como Google, Yahoo, Bing, etc. Estos hacen un seguimiento de cada una de las búsquedas que realizamos, pueden registrar nuestra dirección IP, los términos de búsqueda utilizados, el tiempo de la búsqueda, los destinos elegidos, y mucha más información. Como todos los sitios que recopilan datos, tienen una política de privacidad y es recomendable leerla o por lo menos ojear los conceptos más relevantes. Algo que se aconseja dada esta realidad, es no

ingresar información sensible en las cadenas de búsqueda, como podría ser el número de un documento, teléfono o dirección, hasta la cuenta del banco: la retención de esa cadena significaría que su motor de búsqueda tiene un registro de la misma. ¿Con qué motivo almacenan los buscadores toda esta información? Los argumentos van desde proporcionar mejores servicios y mayor personalización de los resultados a sus usuarios, hasta frustrar amenazas de seguridad y luchar contra los estafadores de clicks. También se utilizan barras de herramientas para la obtención de información acerca de los hábitos de los usuarios.

A raíz de todos estos temas han surgido sitios como el de www.startpage.com, un servicio de búsqueda con sede en los Países Bajos, que no almacena ningún tipo de información de los usuarios. Su política de privacidad fue creada en parte como respuesta a los temores de que si la empresa conserva la información, con el tiempo podría ser mal utilizada, por lo cual llegaron a la conclusión de que si los datos no se almacenan, la privacidad de los usuarios no podría ser violada. Startpage es un meta buscador, es decir, que en sus resultados devuelve los primeros resultados de otros motores de búsqueda.

Una actividad que algunos sitios llevan adelante es el armado del fingerprinting o huella digital de un equipo conectado a la red, se trata de un resumen de la configuración de hardware y software de este. Cada equipo tiene un ajuste de reloj, fuentes, software y otras características que lo hacen único. Existen dos métodos para hacer esta recopilación, uno pasivo utilizando las

características del protocolo TCP, y otro activo mediante algún tipo de código que se instale en el equipo para realizar la recolección de datos.

Cuando el equipo se conecta a Internet, envía toda esta información para los otros componentes de la red o servidores con los que se comunica. Estos datos pueden ser recogidos y ensamblados para formar esta huella digital de forma única para ese dispositivo en particular. Esa huella digital puede ser asignada a un número de identificación, y ser utilizada para fines similares a los que se utiliza una cookie.

Prosiguiendo en este recorrido por los distintos escapes de información personal nos encontramos nuevamente con las redes sociales. Si bien deben ser el punto más conocido por los usuarios, igual digamos que estas son los sitios web que permiten básicamente a los usuarios establecer conexiones y relaciones con otros usuarios de la misma red. Estas redes almacenan información de forma remota, en lugar de hacerlo en el equipo del propio usuario. Los usos que se le pueden dar incluyen el mantenerse en contacto con amigos, hacer nuevos contactos y encontrar gente con intereses e ideas similares, compartir conocimientos, información, experiencias, etc.

Muchas personas además de nuestros amigos y conocidos están interesadas en la información que manejamos en las redes sociales. Reclutadores de talentos, ladrones de identidad, estafadores, cobradores de deudas, acosadores, y las empresas que buscan una ventaja en el mercado están utilizando a las

redes sociales para recopilar información sobre los consumidores. Las empresas motores de redes sociales están recogiendo todos estos datos sobre sus usuarios, tanto para personalizar los servicios como para venderlos a anunciantes.

A modo de ejemplo, dado que anteriormente ya vimos otros, de manera de cuantificar la magnitud y el incremento de la información que circula en las redes sociales de forma pública veamos el caso de Twitter. The Cocktail Analysis reportó en 2008 cómo eran los usuarios de esta red social, que por aquel entonces tenía 3 millones de usuarios únicos, mayormente varones, con interés en la tecnología y generalmente bloggers. Tres años después, las cosas habían cambiado bastante, según lo publicado en el blog oficial de la red social, Twitter contaba con más de 100 millones de usuarios activos, de los cuales más de la mitad se conectaba diariamente para crear algún tweet o seguir sus temas de interés. Como lo han informado, una media de 150 millones de mensajes publicados diariamente en la plataforma. Al comenzar el 2012 existen 500 millones de usuarios en Twitter que comparten unos 300 millones de tweets por día y usan los servicios de esta red de microblogging los medios de comunicación para difundir sus noticias, los famosos para dar a conocer proyectos e informar a sus fans o cualquier usuario con ganas de obtener de primera mano información literalmente acerca de cualquier cosa. Twitter se ha convertido en una plataforma imparable para generar noticias y difundirlas. Así como Jessica Alba anuncia que ha sido madre, Shakira y Piqué suben una foto que confirma su relación o el director de la

Academia de Cine conversa con los internautas a propósito de cierta impopular ley. También los directivos de las compañías realizan sus anuncios a través de esta plataforma, así como presenciamos como Charlie Sheen relanza su carrera luego de una gran controversia.

También encontramos como forma de brindar información personal justamente los sitios Web personales y los blogs, que dependiendo del proveedor del servicio y de los controles o configuración de la privacidad que hagamos, tendrá en mayor o menor medida nuestra información privada disponible públicamente. Si simplemente somos un lector más de un blog y pretendemos hacer un comentario, en algunos casos no nos permitirán hacerlos de forma anónima. De todas formas aunque esto suceda, los sitios pueden registrar datos como la IP de su equipo. Algunos blogs también pueden instalar una cookie buscando asociar todos los comentarios que un usuario ha hecho.

Por otro lado, la banca en línea nos permite tener la posibilidad de verificar saldos en las cuentas o en las tarjetas del banco, transferir dinero entre cuentas, hacer el seguimiento de cheques, etc. Esto nos brinda una gran comodidad, facilitándonos un montón de tareas y ahorrándonos mucho tiempo de espera en largas colas. Los bancos utilizan un sistema de contraseñas y cifrado para proteger su información de acceso y otros tipos de datos sensibles, pero es importante tener cuidado con la información que se comparte o cómo el banco la va a tratar. Cada institución tiene su propia política de privacidad, un consejo

aceptable como siempre es leerla. Depende de nosotros determinar si esa política nos sirve o no, o simplemente poder saber qué va a hacer el banco con nuestros datos. Algunos bancos compartirán parte de su información con terceros con fines de marketing, y es posible encontrar en las políticas de privacidad la forma de hacer un "opt out", notificarle al banco que no deseamos que compartan nuestra información.

Es importante tener cuidado de dar información a la institución adecuada. Muchos sitios Web fraudulentos se han creado semejantes a los sitios reales para intentar realizar phishing. Básicamente se contactan con los usuarios generalmente a través de un mail con esta web falsa y le piden que actualice su información de la cuenta para robar su información personal. Nunca responda a las peticiones no solicitadas por usted con sus contraseñas o números de cuenta, no importa qué tan real parezca ser esa solicitud.

Estos son los medios o los lugares por donde vamos dejando nuestras migajas, rastros de información que pueden ser armados para organizar nuestro ser digital, pero del lado de los proveedores de servicios, de las empresas comerciales y otro tipo de organizaciones o individuos interesados en estos datos.

Por lo tanto, si no tratamos de usar los controles de información personal que están a nuestro alcance existentes en la red, esto nos puede traer algún dolor de cabeza. Pongamos un ejemplo, el perfil de una persona en Facebook contiene fotos y otro tipo de información del ámbito familiar y su círculo de amistades,

información del círculo considerado más personal a diferencia del perfil de la misma persona en Linkedin, donde se comparte la información relacionada al trabajo, aptitudes profesionales, capacidades, conocimientos, etc., todos ellos orientados al ámbito profesional. Si la información almacenada en estos perfiles y la de otros muchos rastros que vamos dejando en la red se mezclan, pueden producirse situaciones no deseadas por el individuo propietario de la misma.

Evidentemente la privacidad de la información es una responsabilidad individual, de cada uno de nosotros, y dependerá de los permisos que concedamos en las redes sociales a las que pertenezcamos para que aparezcan públicamente en un buscador o para ser compartida dentro de la red. Sin embargo, si usted es un usuario frecuente de Internet, se sorprendería de la cantidad de información que puede estar en la red disponible sobre su persona, si quiere ver cuán expuesto está en la red, puede probar servicios de alguna herramienta de búsqueda de personas en Internet como ser 123People.es y ver qué tanto sabe la red sobre usted.

El concepto de "demasiada información personal", es una definición completamente subjetiva y que varía de persona a persona, y entre diferentes grupos generacionales. Por ejemplo, los jóvenes nativos digitales acostumbrados a twittear desde siempre, pueden sentirse más cómodos con esta sobreexposición en la red que aquellas personas adultas, "inmigrantes digitales" en este nuevo mundo.

Hace un tiempo leía acerca de un proyecto interesante: “Por favor Róbenme” (Please RobMe es su nombre original en inglés). El objetivo de este sitio fue sensibilizar a los usuarios sobre el exceso de información que comparten. Decían algo así como, Hey, ¿tiene usted una cuenta de Twitter? ¿Ha notado esos mensajes en los que la gente dice dónde está? Son bastante molestos. Bueno, en realidad son también potencialmente muy peligrosos….

Si bien todos los servicios de geolocalización son muy interesantes y abren un gran abanico de posibilidades para crear algunas aplicaciones o servicios bastante impresionantes y útiles, sin embargo, la forma en la que las personas participan en el intercambio de esta información no es para nada impresionante, o simplemente puede llegar a comprometerlos personalmente. Redes sociales como Foursquare aún siendo una red en la que compartir información con tus contactos, nos permite decirle al mundo dónde nos encontramos mediante la interconexión con nuestros usuarios en otras redes sociales del estilo de Twitter, con actualizaciones que son públicas, y el peligro de decir públicamente donde uno está, radica básicamente en que indirectamente estamos diciendo que nos encontramos en un lugar que definitivamente no es nuestra casa.

Para dar un ejemplo, por un lado dejamos las luces encendidas cuando nos vamos de vacaciones, y por otro lado le estamos diciendo al mundo a través de Internet que no estamos en casa, que hemos viajado y que no volveremos hasta dentro de una

semana. Subimos fotos a Facebook, Twitter y a FourSquare de nosotros y nuestra familia en estas hermosas vacaciones, y dejamos de chequearnos en nuestra casa y en el trabajo, haciendo muy evidente la situación.

El objetivo de este sitio web fue generar conciencia sobre este tema, y que la gente piense acerca de cómo utilizar servicios como Foursquare, Brightkite, etc. El sitio mostraba un mapa con direcciones de las casas con un cartel que indicaba “Please RobMe”, que les ponían luego que recorriendo las redes sociales encontraban, con una aplicación desarrollada por ellos, la información que las personas subían a sus perfiles públicos pudiendo identificar una dirección como sin gente o vacía por cierto período de tiempo. Esto fue sacado de línea en cuanto tuvo un poco de repercusión, porque como dijimos antes no buscaban robar casas sino concientizar a los usuarios sobre el exceso de información compartida en la red. Hay que tener en cuenta que todo el mundo puede obtener esta información haciendo algo tan sencillo como una búsqueda en Twitter o Google y recorriendo a mano las redes sociales.

La privacidad de ubicación es un tema importante, estamos asistiendo a una época donde los sistemas están recopilando y almacenando información de las personas acerca de sus ubicaciones y sus movimientos a lo largo del tiempo. Estos servicios no solo son vía web, por ejemplo tarjetas para peajes automáticos, celulares con GPS, servicios de acceso a Internet por Wi-Fi gratuitos, además de las redes sociales de localización

que usamos cada vez más personas y con mayor frecuencia. Estos sistemas que prometen transformar las interacciones sociales también traen consigo un problema a la privacidad de ubicación. Entendamos por privacidad de ubicación el derecho de un individuo de moverse libremente por lugares públicos sin que esto sea sistemáticamente grabado y almacenado para un posterior uso.

Esto da la posibilidad a las empresas, o a quienes hagan estos registros, saber a donde va una persona, si se reúne con otras, si va a una clínica de salud especializada, hasta si va a la Iglesia. Esta información que antes solo podía ser recogida por un individuo que nos siguiera a todos lados al mejor estilo detective privado, ha pasado a ser recopilada por sistemas ubicuos de dispositivos y aplicaciones.

La realidad nos indica que el rastreo de la ubicación de los usuarios es algo que sucede hoy en día, en 2011 se encontró que el iPhone de Apple recolectaba los datos de ubicación y los almacenaban por un año, si bien Apple publicó un parche para corregir este problema fueron varias las demandas recibidas por la empresa. También se conoció con posterioridad que los teléfonos con sistema operativo Android de Google también recogían estos datos. Luego, en setiembre de 2011, Microsoft fue demandada por hacer seguimiento de los usuarios de teléfonos celulares que venían con el sistema operativo Windows 7. La demanda colectiva presentada ante la Corte Federal de Seattle, acusa a Microsoft de incluir un software que transmite

información, incluidas coordenadas aproximadas de latitud y longitud del dispositivo en cuestión, cuando se activa la aplicación de la cámara, ignorando incluso si el usuario ha solicitado no ser rastreado; a pesar de lo cual la empresa argumentó que sólo recogía la información cuando el usuario había consentido esta situación. Legisladores estadounidenses, en una audiencia pública a la que fueron citados Apple y Google, acusaron a la industria tecnológica de explotar los datos de ubicación con fines de marketing sin tener el adecuado consentimiento de millones de usuarios a los que les estaba haciendo seguimiento.

Las amenazas a la privacidad de ubicación se presentan ocultas en los efectos secundarios de distintos servicios, si bien los beneficios que ofrecen los servicios son importantes, estos deben ser desarrollados o construidos con un eje fuerte en la intimidad de los usuarios y en la protección de esos datos. Los sistemas deben ser desarrollados con un amplio espectro de políticas de privacidad configurables, elegibles por los usuarios, que le permitan incluso ser completamente anónimos, aunque parezca ir contra el sentido de estas redes, por ejemplo los usuarios de móviles quizás no quieran ser rastreados o ubicados por ellas.

Es responsabilidad de los gobiernos procurar como un derecho de sus ciudadanos que la infraestructura que ellos desplieguen para dar diferentes tipos de servicios de ubicación o servicios geográficos se mantenga con un nivel de privacidad alto. Pero también las empresas tienen implicancias importantes en este sentido, éstas tienen razones financieras para diseñar políticas de

privacidad que protejan a sus usuarios, incluyendo costos legales por violaciones a la privacidad en las que pudiesen incurrir, hasta el obtener beneficios de manejar estas políticas como una ventaja competitiva al momento de ofrecer este tipo de servicios.

Un tema que esta en boca de todos en estos últimos tiempos es el cloud computing, o computación en nube. No es que sea un tema nuevo, pero se ha masificado hasta llegar a servicios al usuario final incluso sin costo. Primero que nada veamos de qué se trata; parte del hecho de que las aplicaciones que se cargan en su equipo se ejecutan en algún lugar de la "nube" así como algunos de los servicios que consumimos, desde algún otro servidor al cual accedemos a través de Internet, o desde varios servidores. La nube esta compuesta por cualquier ordenador, servidor, red o sistema, a través del cual la información es trasmitida, procesada y almacenada; y sobre los que los usuarios tienen poco conocimiento directo, además de poca participación y control. Estos servicios se han incrementado de la mano de un acceso a Internet más eficiente con mayores anchos de banda, transformando a la red en una plataforma para tareas informáticas, pudiendo brindar a través de ella la más variada gama de servicios posibles, combinando en la nube software, almacenamiento y poder de cómputo.

Pongamos un ejemplo para ser más claros con estos servicios de computación en nube: con Google Docs tenemos una suite ofimática accesibles desde sus servidores en la red, sus propios servidores, no el nuestro. Así, se puede escribir un documento sin

necesidad de mantener ningún software de procesamiento de textos instalado en nuestro computador. También encontramos servicios de almacenamiento de fotos como Picasa o Flickr, servicios para respaldos de seguridad de nuestros datos y de otras aplicaciones como Mozy o Backupify. Las redes sociales son otro ejemplo de computación en nube, así como las aplicaciones asociadas a estas redes sociales como el juego Farmville, servicios de almacenamiento y reproducción de música como Lastfm o Spotify, u otros de video como Youtube o Netflix, etc. Todos estos servicios vienen listos para usar.

Si bien son muchas las empresas que ofrecen servicios personalizados de computación en nube, los principales actores en este mercado son Google, Amazon, Microsoft, IBM, Salesforce, Yahoo, Sun, Oracle, EMC, Intuit, etc. Estos también presentan soluciones para empresas, que pueden ir desde adquirir tu propia solución de nube privada o utilizar los servicios de estos proveedores.

Buenos servicios, bajas inversiones, acceso a tecnología que muchas veces no es posible adquirir por parte de los usuarios, pero tenemos que conocer cuáles son los riesgos del cloud computing o qué debemos leer y conocer para mitigarlos o manejarlos correctamente. El primer problema que puede pensarse existe en la computación en nube es la pérdida de cierto nivel de control sobre la información, que podría llegar a ser confidencial. Según encuestas hechas en la red Linkedin, más de la mitad de las personas dice que el riesgo principal en este

campo es la seguridad de la información. En este escenario, la responsabilidad de proteger la información frente a posibles violaciones internas y/o externas de la seguridad, queda mayormente en manos de la empresa proveedora del servicio y no del cliente y dueño de la información, más allá del manejo correcto de usuario y clave. Por este motivo, y nuevamente como en todos los servicios de Internet, es fundamental la lectura de la política de privacidad y de los términos del servicio. Estos documentos proporcionan una cantidad de información valiosa sobre el tratamiento que tendrán nuestros datos. Otro punto a tener en cuenta es la localización geográfica del proveedor, esto tendrá una variación en la legislación aplicable ante cualquier conflicto sobre la responsabilidad de una violación de seguridad o divulgación de la información.

Una opción para todos estos servicios, redes sociales, computación en nube, geolocalización, etc., debería ser incluir en las políticas de uso, períodos de mantenimiento de información, adicionalmente al uso o fin que se le dará a la misma por parte del prestador del servicio, aclarar cuanto tiempo se almacenarán los diferentes tipos de datos, alguien que geolocaliza la posición de tu móvil durante cuánto tiempo tendrá esa información almacenada, o incluso el tiempo que se mantendrán las búsquedas que has hecho en la web, esto debe quedar estipulado como forma de proteger tu privacidad.

Entre algunos riesgos que corren los usuarios y a los que debemos estar atentos, está el hecho de que los sitios pueden

cambiar sus políticas, de una posición de borrado a otra de retención. También pueden aparecer leyes que obliguen a mantener la información almacenada por una cantidad de tiempo alegando ser necesarios por temas gubernamentales e incluso llegando a argumentar su necesidad para la defensa nacional, como ya se ha manejado en Estados Unidos y en Europa.

La necesidad de mantener la privacidad y de cuidar que cierta información no se comparta es una concepción que debemos preservar individualmente, nadie quiere que sus empleados o empleadores sepan cosas de su vida tan personales como cuando va a la iglesia, que sus compañeros sepan cuando está de fiesta o lo que hace en ella, o si va de compras y menos qué compra, que sus ex parejas sepan cuándo esta con su actual pareja o dónde van de vacaciones, ni que la competencia de su empresa pueda conocer la ubicación y la información que comparte la fuerza de venta de su negocio entre si.

Para todo esto debemos poner atención en nuestra privacidad, revisar las configuraciones, conocer las reglas con las que funcionan los sitios web de los cuales consumimos los diferentes servicios, pero también tener cuidado en lo que subimos, las fotos que compartimos, los comentarios que hacemos y con quienes los compartimos. Cada vez más las redes sociales permiten hacer grupos o restricciones a la hora de compartir información, pero esta puede ser reenviada por nuestros contactos, así que si no queremos que todo el mundo se entere de algo, quizás sea mejor no subirlo…

9. FUENTES DE INFORMACIÓN

Organizaciones sin fines de lucro:

Privacy Rights Clearinghouse
Dándole poder a los consumidores, protegiendo la privacidad.
http://www.privacyrights.org/

The Electronic Frontier Foundation
Defendiendo tus derechos en un mundo digital.
http://www.eff.org/

INSAFE
Red Europea de Centros de Sensibilización para el uso seguro y responsable de Internet y dispositivos móviles para los jóvenes.
http://www.saferinternet.org/

PEW Internet
Información sobre temas de Internet, actitudes y tendencias. Forma parte de The Pew Research Center.
http://www.pewinternet.org/

Foro Generaciones Interactivas
Inclusión de la familia, la escuela y la sociedad. Uso y posesión de las TIC's entre niños y adolescentes en Iberoamérica.
http://www.generacionesinteractivas.org/

Pantallas Amigas
Promoción, Participación y Protección de la Infancia y la Adolescencia en Internet y otras Tecnologías Online
http://pantallasamigas.net

ACLU OF MARYLAND
Fundación Americana de Libertades Civiles del estado de Maryland
http://www.aclu-md.org/

Centros de Enseñanza:

Universidad de Maryland at Baltimore.
Departamento de Ciencias de la Computación e Ingeniería Eléctrica http://ebiquity.umbc.edu/

Universidad de Maryland.
Grupo de aprendizaje en Estadística Relacional
http://linqs.cs.umd.edu/

University of Texas at Dallas
http://www.utdallas.edu/

University of British Columbia
Facultad de Ciencias Aplicadas. Departamento de Ingeniería Eléctrica y Computación.
http://www.ece.ubc.ca/

Medios de Prensa:

Wall Street Journal (EE.UU.)
http://online.wsj.com/

New York Times (EE.UU.)
http://www.nytimes.com

The Huffington Post (EE.UU.)
http://www.huffingtonpost.com/

TIC Beat (España)
http://www.ticbeat.com/

Read Write Web (EE.UU.)
http://www.readwriteweb.com/

La Vanguardia (España)
http://www.lavanguardia.com/

PC World (EE.UU.)
http://www.pcworld.com/

The Guardian (Inglaterra)
http://www.guardian.co.uk

Folha SP (Brasil)
http://www.folha.uol.com.br/

NoticiasDot (España)
http://www.noticiasdot.com/

The Atlantic (EE.UU.)
http://www.theatlantic.com/

Blogs y Otros:

Branding - Andy Stalman
http://www.tendencias21.net/branding/

Enrique Dans
http://www.enriquedans.com/

Nik Cubrilovic
http://nikcub.appspot.com/

Viktor Mayer-Schönberger
http://www.vmsweb.net/

Alberto Ortiz de Zárate Tercero

http://alorza.wikispaces.com/

Saskia Sassen
http://es.wikipedia.org/wiki/Saskia_Sassen

William J. Mitchell
http://web.media.mit.edu/~wjm/

Dr. Paco Traver
http://pacotraver.wordpress.com/

INSIDEFACEBOOK - Uso y Crecimiento de Facebook
http://www.insidefacebook.com/

DE LO PRIVADO A LO PÚBLICO.

El auge de la Web 2.0 y la relación de nuestras vidas con la red han llevado a manejar la idea de El Yo Digital como parte de nuestra identidad.

El peligro de la Privacidad es la gradual erosión de las libertades individuales a través de la automatización, integración e interconexión de sistemas pequeños y separados de mantenimiento de registros.

La red toca casi todos los aspectos de nuestras vidas, y la información que compartimos en ella es responsabilidad de cada individuo, compartir demasiada información personal puede bajo ciertas circunstancias o usos resultar ser incómodo o inaceptable.